



NIS2 Directive: EU-wide Obligations

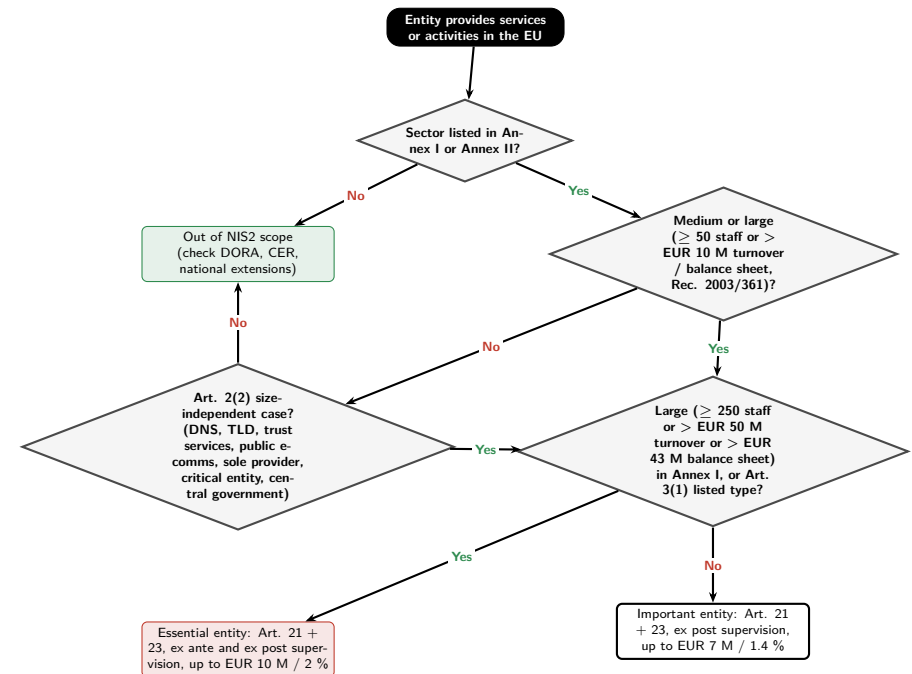
Directive (EU) 2022/2555, in force 16 Jan 2023, transposition due 17 Oct 2024 | Scope, Art. 20-21 measures, Art. 23 reporting, supervision, fines, links to DORA / CER / CRA

#NIS2 #EURegulation #RiskManagement #IncidentReporting

What NIS2 is and who is in scope

INFO

NIS2 (second Network and Information Security directive) replaces NIS 1 (Directive 2016/1148) from 18 October 2024. It is a **directive**: each member state transposes it into national law, so authorities, registration portals, registration deadlines and exact fines vary by country. In France the authority is **ANSSI** (Agence nationale de la sécurité des systèmes d'information, the national cyber agency); NIS2 there extends the old OIV (opérateurs d'importance vitale, vital operators) and OSE (opérateurs de services essentiels, NIS 1 operators of essential services) regimes to thousands of entities through a resilience bill (projet de loi résilience). This sheet covers the EU text itself (the ANSSI governance track adds French detail). Companion acts: **CER** Directive 2022/2557 (Critical Entities Resilience: physical, all-hazards resilience), **DORA** Regulation 2022/2554 (Digital Operational Resilience Act for finance, a *lex specialis*: a more specific law that prevails), **CRA** Regulation 2024/2847 (Cyber Resilience Act: security of products). **ENISA** = EU Agency for Cybersecurity; **CSIRT** = Computer Security Incident Response Team.



Essential entities (EE), Art. 3(1)	Important entities (IE), Art. 3(2)
large entities in Annex I high-criticality sectors	medium entities in Annex I; medium and large entities in Annex II
regardless of size: qualified trust service providers, TLD registries, DNS service providers; medium-sized public electronic communications providers; central government public administration; critical entities under CER; former NIS 1 operators of essential services	any entity in Annex I or II that is not essential; entities designated by a member state under Art. 2(2)(b)-(e) as important
Art. 32: ex ante and ex post supervision: on-site inspections, regular and targeted audits, ad hoc audits, security scans, information and evidence requests	Art. 33: ex post only, triggered by evidence, indication or information of non-compliance
Art. 34(4): up to EUR 10 M or 2 % of worldwide annual turnover, whichever is higher	Art. 34(5): up to EUR 7 M or 1.4 %, whichever is higher
Art. 32(5): temporary suspension of certification or authorisation; temporary ban on CEO or legal representative from managerial functions	no suspension or ban powers; same corrective orders and fines
Annex I: sectors of high criticality (11)	Annex II: other critical sectors (7)
Energy: electricity (incl. producers, distribution and transmission system operators (DSO, TSO), charging point operators), district heating and cooling, oil, gas, hydrogen	Postal and courier services
Transport: air, rail, water, road (operators of intelligent transport systems, ITS: traffic management and control)	Waste management
Banking: credit institutions (DORA applies instead of Art. 21 and 23)	Manufacture, production and distribution of chemicals
Financial market infrastructures: trading venues, CCPs (DORA)	Production, processing and distribution of food
Health: healthcare providers, EU reference laboratories, pharma R&D, manufacturers of basic pharmaceutical products and medical devices critical in a public health emergency	Manufacturing: medical devices and in vitro diagnostics, computer/electronic/optical products, electrical equipment, machinery, motor vehicles and trailers, other transport equipment
Drinking water; Waste water (when essential part of the activity)	Digital providers: online marketplaces, online search engines, social networking platforms
Digital infrastructure: internet exchange points (IXP), DNS providers, top-level domain (TLD) registries, cloud, data centres, content delivery networks (CDN), trust service providers (e-signatures, certificates), public electronic communications networks and services	Research organisations
ICT service management (business to business): managed service providers (MSP: run IT for clients), managed security service providers (MSSP: run SOC, monitoring)	
Public administration: central government; regional at member state choice	
Space: operators of ground-based infrastructure	

EXAM TIP

Trap: size is the **default** criterion, not the only one. A five-person DNS provider or qualified trust service provider is an essential entity. Conversely, a large bank is in Annex I but follows **DORA** for measures and reporting (NIS2 Art. 4 sector-specific acts). Micro and small entities are out unless an Art. 2(2) condition applies.

Governance and the ten minimum measures (Art. 20-21)

Art. 20 Governance: management bodies
must **approve** the cybersecurity risk-management measures, **oversee** their implementation and **can be held liable** for infringements; must **follow training** and should offer similar training to employees regularly. Liability and training are the two exam keywords.

Art. 21(1) all-hazards approach
appropriate and proportionate technical, operational and organisational measures; proportionality judged on exposure, size, likelihood and severity of incidents including societal and economic impact; state of the art and European or international standards (ISO/IEC 27001, ETSI) taken into account.

Art. 21(4) corrective action
an entity that finds it does not comply must take all necessary, appropriate and proportionate corrective measures **without undue delay**.

Art. 21(2) minimum measures (a)-(j), all mandatory

✓ Art. 21(2) item; note = evidence an auditor or supervisor expects

- ✓ (a) Policies on risk analysis and information system security documented risk assessment method (ISO/IEC 27005 or EBIOS RM, the ANSSI risk method), ISMS (information security management system) policy, defined scope
- ✓ (b) Incident handling incident response (IR) plan, 24/7 on-call, playbooks, runbook that starts the Art. 23 reporting clocks
- ✓ (c) Business continuity, backup management, disaster recovery, crisis management offline or immutable backups, tested restores, BIA (business impact analysis: which services, how fast), crisis cell
- ✓ (d) Supply chain security, including relationships with direct suppliers and service providers supplier risk tiering, contract clauses, Art. 22 coordinated EU risk assessments
- ✓ (e) Security in acquisition, development and maintenance, including vulnerability handling and disclosure SSDLC (secure software development life cycle), patch deadlines (SLAs), CVD (coordinated vulnerability disclosure) policy; Art. 12 national CVD coordinator, ENISA EU vulnerability database (EUVD, live since May 2025)
- ✓ (f) Policies and procedures to assess the effectiveness of the measures KPIs (key performance indicators), internal audits, penetration tests, management review minutes
- ✓ (g) Basic cyber hygiene practices and cybersecurity training hardening, least privilege, awareness programme with records
- ✓ (h) Policies and procedures on cryptography and, where appropriate, encryption crypto policy (approved algorithms, key lengths), key management, PQC (post-quantum cryptography) migration roadmap
- ✓ (i) Human resources security, access control policies and asset management joiner-mover-leaver process (grant, change, revoke access), periodic access reviews, asset inventory

✓ (j) MFA or continuous authentication, secured voice, video and text communications, secured emergency communication systems MFA (multi-factor authentication) on remote access and admin accounts, encrypted messaging, out-of-band crisis channel that survives loss of email

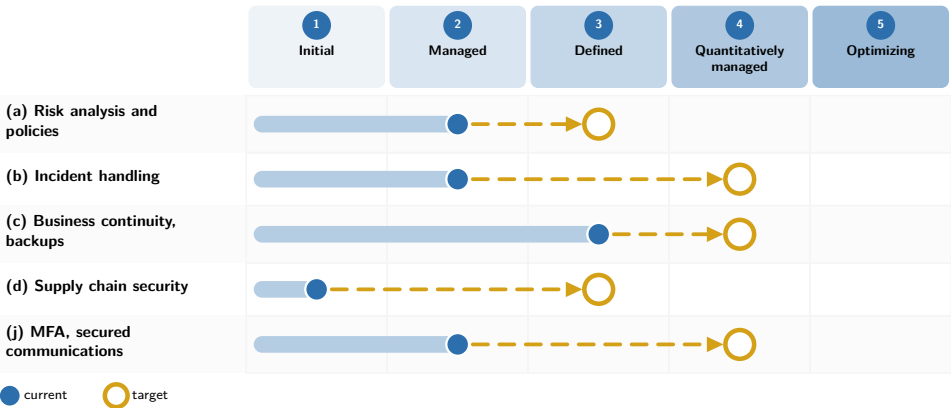
TIP

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 details the Art. 21(2) measures and the significance thresholds of incidents for DNS providers, TLD registries, cloud, data centres, CDNs, managed (security) service providers, online marketplaces, search engines, social networks and trust service providers (Art. 21(5) mandate). Its annex reads like an ISO 27001 control set with explicit review periods; use it as the de facto EU baseline even outside those sectors (thresholds: verify against the text).

Task	Management body	CISO	Business owners	Staff
Approve Art. 21 measures	A	R	C	
Oversee implementation	A	R	R	
Cyber training (Art. 20(2))	R	A		R
Report significant incidents	I	A	C	

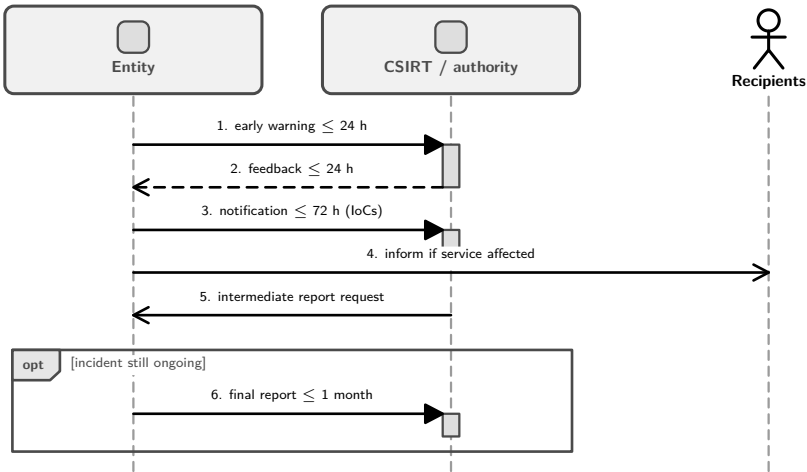
R Responsible A Accountable C Consulted I Informed

Art. 20 in RACI form: the management body approves the Art. 21 measures, oversees their implementation, must follow training and can be held liable for infringements (A = accountable, R = responsible, C = consulted, I = informed)



Art. 21(2) readiness of a newly in-scope important entity (levels 1 initial to 5 optimising; current values illustrative): the dashed arrows are the gaps the management body must fund and oversee

⚠ Incident reporting (Art. 23)



Art. 23 reporting as an exchange: the clocks run from awareness of a significant incident; the CSIRT or authority answers the early warning within 24 h with feedback and, on request, guidance (Art. 23(5))

Significant incident (Art. 23(3)) — has caused or is capable of causing severe operational disruption of the services or financial loss for the entity, or has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

Recipients of services (Art. 23(1)-(2)) — entities inform recipients of their services likely to be affected by a significant incident without undue delay, and of measures they can take in response to a significant cyber threat

Voluntary notification (Art. 30) — any entity may report incidents, cyber threats and near misses; does not create extra obligations

Public information (Art. 23(7)) — the authority may inform the public or require the entity to do so when public awareness is necessary

⚠ WARNING

Reporting to the CSIRT does **not** replace GDPR Art. 33 (72 h to the data protection authority), DORA, or sector notifications. The authority forwards cross-border incidents to other member states and to ENISA (Art. 23(6)); ENISA publishes a biannual summary. Feedback and guidance from the CSIRT come within 24 h of the early warning (Art. 23(5)).

🕒 Supervision, cooperation and timeline

10 M / 2 %

essential entities max fine

Art. 34(4), whichever higher

7 M / 1.4 %

important entities max

fine

Art. 34(5)

24 / 72 / 30

hours, hours, days

Art. 23 early warning, notification,
final report

18

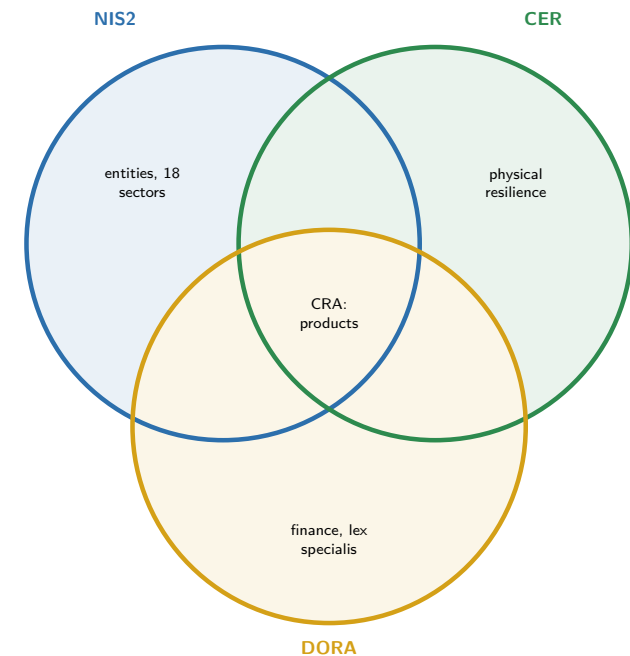
sectors

11 Annex I + 7 Annex II

NIS2 next to DORA, CER and CRA

2022-12-14	Adoption — NIS2 adopted; published in the OJ on 27 December 2022, in force 16 January 2023
2024-10-17	Transposition deadline — member states must adopt and publish national measures; Implementing Regulation 2024/2690 adopted the same day; NIS 1 repealed 18 October 2024
2024-10	Belgium, Italy, Croatia, Hungary, Lithuania among the first — Belgium: law of 26 April 2024 (CCB as authority); Italy: decreto legislativo 138/2024 (ACN); most other states late
2024-11-28	Infringement procedures — Commission sends letters of formal notice to 23 member states for failing to transpose; reasoned opinions to 19 states on 7 May 2025
2025-01-17	ENISA registry — Art. 27: DNS, TLD, cloud, data centre, CDN, MSP/MSSP, marketplace, search engine and social network providers submit registration data
2025-04-17	Lists of entities — Art. 3(3): member states establish the list of essential and important entities, reviewed at least every two years
2025-12	Germany — NIS2UmsuCG promulgated 5 Dec 2025 (BGBl. 2025 I Nr. 301), in force 6 Dec 2025 (BSI as authority), about 14 months late; France: resilience bill (loi resilience) transposing NIS2, CER and DORA adopted by the Senate on 12 Mar 2025, National Assembly debate scheduled for Oct 2026, not yet promulgated in Sept 2026
2027-10-17	Review — Art. 40: Commission reviews the functioning of the directive, then every 36 months

Art. 8-11	competent authorities, single point of contact (SPOC), CSIRTs and their tasks (monitoring, early warning, forensics, CVD coordination)
Art. 12	coordinated vulnerability disclosure: national CSIRT as coordinator; ENISA European vulnerability database
Art. 14-16	Cooperation Group, CSIRTs network, EU-CyCLONe (large-scale crisis management network)
Art. 22	coordinated security risk assessments of critical supply chains (e.g. 5G toolbox approach)
Art. 31-37	supervision and enforcement; Art. 35 GDPR interplay: authorities inform data protection authorities when a breach involves personal data



- **CER 2022/2557** all-hazards resilience of critical entities in 11 sectors; a CER critical entity is automatically an NIS2 essential entity (Art. 3(1)(f))
- **DORA 2022/2554** replaces NIS2 Art. 21 and 23 for financial entities; NIS2 authorities and financial supervisors exchange information
- **CRA 2024/2847** secures the products entities buy; Art. 21(2)(e) vulnerability handling and the CRA SBOM / CVD duties meet at procurement

Aspect	NIS2	DORA	CRA
Object	entities (organisations)	financial entities and critical ICT providers	products with digital elements
Type of act	directive (transposed)	regulation (direct)	regulation (direct)
First report	24 h early warning	4 h after classifying as major, ≤ 24 h after awareness (RTS: regulatory technical standards)	24 h early warning to the ENISA single reporting platform
Max fine	10 M / 2 % (EE), 7 M / 1.4 % (IE)	set by member states; periodic penalty on a critical ICT third-party provider (CTPP) up to 1 % of average daily worldwide turnover	15 M / 2.5 %
Applies	18 Oct 2024 (national dates vary)	17 Jan 2025	reporting 11 Sep 2026, full 11 Dec 2027

Obligation (CRA: manufacturer duty)	NIS2	DORA	CRA	ISO 27001:2022
Management body approves and is accountable	Art. 20	Art. 5(2), 5(4)	✗	cl. 5.1, 5.3
Supplier and component risk	Art. 21(2)(d), 21(3)	Art. 28-30	Art. 13(5) due diligence	A.5.19-5.23
Vulnerability handling and disclosure	Art. 21(2)(e), Art. 12 CVD	Art. 9-10 (partial)	Annex I Part II, SBOM	A.8.8
Resilience testing beyond audits	Art. 21(2)(f)	Art. 24-27, TLPT every 3 years	Annex I Part II(3)	cl. 9.2, A.8.29
Register kept for the supervisor	registration data (Art. 3(4), 27)	register of information (Art. 28(3))	technical file ≥ 10 years (Art. 13(13))	Statement of Applicability (cl. 6.1.3)

✓ covered ◯ partly covered ✗ not covered

≡ Mapping Art. 21(2) to ISO 27001 and a reporting drill

📘 INFO

How to read the mapping: ISO/IEC 27001:2022 **clauses 4-10** are the management-system requirements (6.1.2 risk assessment, 6.1.3 risk treatment, 7.2 competence, 7.3 awareness, 8.2-8.3 performing assessment and treatment, 9.1 monitoring, 9.2 internal audit, 9.3 management review); **Annex A** lists 93 controls in 4 themes (A.5 organisational, A.6 people, A.7 physical, A.8 technological). NIST CSF 2.0 ids are Function.Category (GV Govern, ID Identify, PR Protect, DE Detect, RS Respond, RC Recover).

Art. 21(2) measure	ISO/IEC 27001:2022 clauses and Annex A controls	NIST CSF 2.0 categories
(a) risk analysis, IS policies	6.1.2 risk assessment, 6.1.3 treatment, 8.2-8.3; A.5.1 policies for information security	GV.RM risk strategy, ID.RA risk assessment
(b) incident handling	A.5.24-5.28 incident planning, triage, response, lessons learned, evidence; A.6.8 event reporting by staff; A.8.16 monitoring	RS.MA incident management, RS.AN analysis, DE.AE adverse-event analysis
(c) BC, backup, DR, crisis	A.5.29 security during disruption, A.5.30 ICT readiness for continuity, A.8.13 backup, A.8.14 redundancy	RC.RP recovery plan execution, PR.IR infrastructure resilience
(d) supply chain	A.5.19-5.23 supplier relationships, agreements, ICT supply chain, supplier monitoring, cloud services	GV.SC supply chain risk management
(e) acquisition, development, vulnerability handling	A.8.8 technical vulnerabilities, A.8.25-8.29 secure SDLC, requirements, architecture, coding, testing; A.8.32 change management	ID.RA, PR.PS platform security
(f) effectiveness assessment	9.1-9.3 monitoring, internal audit, management review; A.5.35 independent review, A.5.36 compliance checks	ID.IM improvement, GV.OV oversight
(g) cyber hygiene, training	7.2-7.3; A.6.3 awareness and training, A.8.1 endpoints, A.8.7 anti-malware, A.8.9 configuration management	PR.AT awareness and training, PR.PS
(h) cryptography	A.8.24 use of cryptography (policy, key management)	PR.DS data security
(i) HR security, access control, assets	A.5.9-5.18 asset inventory to access rights, A.6.1-6.5 screening to post-employment, A.8.2 privileged access, A.8.3 access restriction	PR.AA identity and access, ID.AM asset management
(j) MFA, secured communications	A.5.14 information transfer, A.5.17 authentication information, A.8.5 secure authentication, A.8.20-8.21 network security	PR.AA, PR.DS

📘 NOTE

An ISO 27001 certificate is strong evidence but **not** automatic NIS2 compliance: scope may exclude the service in question, Art. 20 management training and liability, Art. 23 clocks and national registration are outside the standard. Some transpositions (e.g. Belgium with Cyber-Fundamentals or ISO 27001 conformity) accept certification as a presumption for supervision (verify per country).

📄 EXAMPLE

Drill: Friday 18:00 a managed service provider detects ransomware encrypting customer-facing hypervisors. **Saturday 18:00** latest: early warning to the CSIRT (malicious act suspected, possible cross-border impact as customers sit in three member states). **Monday 18:00**: incident notification with initial severity, impact and IoCs; inform affected customers (Art. 23(1)). GDPR clock runs in parallel if personal data is affected (72 h, the DPA). **Within one month** of the notification: final report with root cause and mitigation, or a progress report if still ongoing.

Mnemonic: **PIBSEF-HCHM**

- P** Policies on risk (a)
- I** Incident handling (b)
- B** Business continuity (c) backup, DR, crisis
- S** Supply chain (d)
- E** Engineering security (e) acquisition, development, vulnerability disclosure
- F** Follow-up of effectiveness (f)
- H** Hygiene and training (g)
- C** Cryptography (h)
- H** HR, access, assets (i)
- M** MFA and secure comms (j)

🕒 When is an incident significant? (Implementing Regulation 2024/2690)

For the digital providers it covers (DNS, TLD, cloud, data centres, CDN, MSP/MSSP, marketplaces, search engines, social networks, trust services), the regulation turns the vague Art. 23(3) test into numbers. One criterion met = significant = the 24 h / 72 h / 1 month clocks apply. Values below are from Art. 3-4 and the provider-specific articles (verify exact wording before use).

Criterion	Threshold that makes it significant	Scope
Direct financial loss	> EUR 500 000 or > 5 % of annual turnover, whichever is lower	all providers
Trade secrets	exfiltration of trade secrets (Directive 2016/943)	all providers
People	death of a natural person, or considerable damage to health	all providers
Intrusion	successful, suspected malicious and unauthorised access able to cause severe operational disruption	all providers

Recurring incidents	same apparent root cause at least twice in 6 months, together meeting the financial criterion (Art. 4)	all providers
Service down	cloud service completely unavailable > 30 min, or degraded for > 5 % of EU users (or > 1 M users) for > 1 h	cloud
Name resolution	recursive or authoritative DNS resolution unavailable > 30 min	DNS

- 1 Scope and classify run the decision tree per legal entity: sector (Annex I or II), size, Art. 2(2) cases; result = essential, important or out
- 2 Register national portal (and the ENISA registry for Art. 27 digital providers): name, sector, contacts, IP ranges, member states served
- 3 Train and mandate the board Art. 20 training for management, approval of the risk-management measures recorded in minutes
- 4 Gap analysis against Art. 21(2) (a)-(j) use Implementing Regulation 2024/2690 annex or ISO 27001 Annex A as the checklist; prioritise MFA, backups, supplier clauses
- 5 Reporting runbook who decides significance, who files the 24 h early warning, CSIRT contacts, parallel GDPR and DORA clocks, templates ready
- 6 Measure and improve Art. 21(2)(f): KPIs, internal audit, management review; keep evidence for ex ante (essential) or ex post (important) supervision

A first-year NIS2 programme (typical order)

Common NIS2 mistakes vs good practice

✓ Good practice	✗ Common mistake
+ classify each legal entity of a group separately (size is counted per enterprise with partner and linked companies, Rec. 2003/361)	– assuming small size exempts a DNS, TLD or qualified trust provider
+ treat supplier security as contract clauses plus evidence (audit rights, incident notification to you, SBOM)	– waiting for root cause before the early warning (24 h needs only suspicion of malice and cross-border impact)
+ rehearse the 24 h early warning on a Friday-night scenario	– treating an ISO 27001 certificate as NIS2 compliance

Essential entity (EE) — NIS2 category with the heaviest regime: large Annex I entities plus size-independent cases; proactive (ex ante) supervision and EUR 10 M / 2 % fines.

Important entity (IE) — Any other in-scope NIS2 entity; same measures and reporting, reactive (ex post) supervision and EUR 7 M / 1.4 % fines.

Lex specialis — A more specific law that prevails over a general one for the same subject (DORA over NIS2 for finance, NIS2 Art. 4).

Early warning — NIS2 Art. 23(4)(a) first notice to the CSIRT within 24 h of awareness of a significant incident.

✓ Self-test

- Q1 How many Art. 21(2) minimum measures, and which letter covers MFA?
A Ten, (a) to (j); MFA and secured communications are (j)
- Q2 Early warning deadline and what it must state?
A 24 h after awareness: whether malicious or unlawful act is suspected and whether cross-border impact is possible
- Q3 Who is essential regardless of size?
A Qualified trust service providers, TLD registries, DNS service providers (plus central government, CER critical entities, medium public e-comms providers)
- Q4 Supervision difference EE vs IE?
A EE: ex ante and ex post (inspections, audits, scans); IE: ex post only on evidence of non-compliance
- Q5 Is an ISO 27001 certificate proof of NIS2 compliance?
A No: strong evidence for Art. 21, but scope, Art. 20 governance duties, Art. 23 reporting and national registration must be shown separately
- Q6 Which Art. 21(2) letter covers vulnerability handling and disclosure?
A (e) security in acquisition, development and maintenance, including vulnerability handling and disclosure