Copla

NIS 2

Compliance Explainer

Table of contents

What NIS 2 is and why it matters now

NIS 2 (Directive (EU) 2022/2555) is the EU's updated cybersecurity baseline for "essential" and "important" entities operating in critical sectors. It expands the original NIS and establishes clearer obligations for risk management, incident reporting, and governance, backed by stronger supervision and increased fines.

The directive is in force and applies through your national law; Member States must identify essential entities and keep those lists updated (the first lists are due by 17 April 2025).

Why it matters

- Your leadership is now directly accountable.
- Incident reporting clocks are unforgiving (hours/days, not weeks).
- Supply-chain security is explicit and auditable.
- Fines reach €10m / 2% (essential) and €7m / 1.4% (important).

Who is in scope?

NIS 2 covers medium+ organizations (≥50 employees or ≥€10m turnover) in Annex I (essential) and Annex II (important) sectors, plus smaller ones whose disruption is critical. Both share the same baseline security and reporting duties. Essential entities face proactive (ex-ante/ex-post) supervision; important entities mainly ex-post.

Essential entities

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

Important entities

- Postal and courier services
- Waste management
- Manufacture, production & distribution of chemicals
- Food production, processing & distribution
- Manufacturing
- Digital providers
- Research organisations

NIS 2 vs DORA: Which applies to financial entities (2025)

If you're regulated under EU financial services law, DORA applies in parallel to NIS 2 and takes precedence where both cover ICT risk/operational resilience.

- Lex specialis & scope: DORA (Reg. (EU) 2022/2554) is sector-specific; it supersedes NIS 2 in terms of ICT risk, incident reporting, resilience testing, and third-party ICT risk.
- Supervision: Overlapping ICT-resilience areas are overseen by financial supervisors (EBA/ESMA/EIOPA/nationals), not NIS 2 authorities.
- ICT providers: Non-financial ICT firms serving the finance sector may be designated as critical ICT third parties and fall under EU-level oversight.
- Direct & timed: A directly applicable regulation (no transposition), in force since 2023 and applicable from 17 Jan 2025 (near NIS 2 identification after the 17 Oct 2024 transposition).
- Practical takeaway: For financial entities, DORA governs ICT resilience; NIS 2 may still apply to broader cybersecurity/supply-chain duties.

Copla cross-maps NIS 2 and DORA, so you implement once and satisfy both.

What you must do

Article 21 requires appropriate and proportionate cybersecurity measures, covering at least the domains listed below. These maps cleanly align with ISO/IEC 27001 controls, which is why many teams use ISO 27001 as the operating backbone.

1. *Risk analysis & information security policies*
2. *Incident handling*
3. *Business continuity incl. backup/DR & crisis mgmt*
4. *Supply-chain security (incl. Article 21(3) supplier oversight)*
5. *Secure acquisition, development & maintenance (incl. vuln mgmt)*
6. *Effectiveness measurement of cybersecurity measures*
7. *Basic cyber hygiene & training*
8. *Cryptography & encryption policies*
9. *Human resources security*
10. *Access control & asset management*
11. *Multi-factor/continuous auth & secured comms*
12. *Logging & detection*
13. *Cross-cutting governance, documentation, proportionality*

Incident reporting

Under Article 23, significant incidents must be reported on a strict timeline:

Early warning

Within 24h of awareness (flag malicious/cross-border if known)

Incident notification

Within 72h with initial impact & IOCs

Final report

Within 1 month (root cause, severity, mitigation, progress)

Governance: board accountability and training

Article 20 makes management bodies responsible for approving cybersecurity measures, overseeing implementation, and states that they can be held liable for infringements of Article 21. It also requires regular training for management and staff.

Supervision & penalties

Competent authorities can request information/evidence, conduct on-site and off-site checks, and audits. Non-compliance can lead to warnings, binding instructions with deadlines, and fines. The competitor summary (p.12) lists these layers succinctly.

Administrative fines: *(Article 34)*

Essential entities

Up to €10 m or 2% of global annual turnover (whichever is higher).

Important entities

Up to €7 m or 1.4% of global annual turnover (whichever is higher).

The manual compliance burden (without automation)

First-time NIS 2 readiness in a cloud-first mid-size organization commonly requires ~820–1,120 internal hours over 6–9 months. Below is a representative split (excludes pen tests, SIEM tuning, or major vendor remediation):

~400–550h

ISMS backbone (ISO-aligned) — policies, risk, SoA, continuity.

~180–260h

Technical controls — MFA, backups, logging/monitoring, access reviews.

~120–180h

Supply-chain security — due diligence, contracts, attestations, monitoring.

~80–120h

Incident reporting program — playbooks, exercises, templates (24h/72h/30d)

~40–60h

Governance & training — board briefings, role assignments, management review.

Ongoing run-state: budget ~20–30h/quarter to keep reviews, evidence, and vendor attestations current.

Indicative internal cost (blended €6k–€8k/mo per FTE): €60k–€120k.

NIS 2 compliance is 40–70% faster with Copla.

Time & cost by organization size (first-time readiness)

Benchmarks assume a typical SaaS/tech stack; your mileage varies with scope and maturity.

Org size	< 50 people	50–150 people	150+ people
Timeline	4–6 months	6–8 months	8–12 months
Internal effort	€40k+ equivalent	€80k+ equivalent	€120k+ equivalent
Indicative internal cost*	€40k–€60k	€80k–€100k	€120k–€180k

* Internal cost bands reflect blended FTE costs and do not include external tests/tools where required.

With Copla, teams typically cut time and internal costs by 40–70%, while improving audit-readiness.

Where the burden spikes

Article 21 requires appropriate and proportionate cybersecurity measures, covering at least the domains listed below. These maps cleanly align with ISO/IEC 27001 controls, which is why many teams use ISO 27001 as the operating backbone.

Vendors & supply-chain

Getting usable assurances, contractual clauses, ongoing monitoring, and corrective action workflows

Evidence management

Proving the 13 domains with living records (access reviews, change logs, DR tests, training).

Incident pipelines

Building the 24h/72h/30d muscle memory.

Exec accountability

Briefings, sign-offs, and cadence.

How Copla reduces cost & time

Platform accelerators

- **Pre-mapped NIS 2 playbook:** Tasks aligned to Articles 20/21/23 with editable policy packs, role assignments, and evidence checklists.
- **Evidence automation:** Track access reviews, training logs, vendor attestations, backup tests, and incident reports in one place; generate audit-ready reports on demand.
- **ISO-aligned templates & controls:** SoA, risk workflows, continuity & incident runbooks, MFA/ encryption baselines — cross-mapped to your stack.

Typical outcomes

- **40–70%** faster time-to-readiness and **40–70%** lower internal compliance cost.
- **50–80% less manual paperwork** for vendor management through reusable clauses, attestations, and a dynamic Register of Information.
- **2× better audit-readiness** (measured by evidence completeness on first pass).

Estimated hours by the NIS 2 area

	without Copla	with Copla
ISMS core (ISO-aligned)	400–550h	200–320h
Technical controls (MFA, logging, backups)	180–260h	90–150h
Supply-chain security	120–180h	50–90h
Incident reporting	80–120h	35–60h
Governance & training	40–60h	20–35h
Total	~820–1,120h	~395–655h

A phased, practical path to compliance

Phase 1 — Mobilize (Weeks 1–3)

- Confirm scope and applicability via size-cap, sector, and national law; identify if DORA applies instead.
- Stand up an ISMS workspace; assign owners for each NIS 2 domain.
- Start risk register and asset inventory; select ISO-aligned policies (access, backup/BCP, incident, vendor, crypto).

Phase 2 — Implement (Weeks 4–10)

- Close the top policy & control gaps across the 13 domains (MFA, logging, backups, DR runbooks, supplier due diligence, vulnerability handling).
- Build incident reporting workflow (24/72/30)—decision trees, templates, roles, comms, and dry-runs.
- Launch training (exec + staff) and secure management approval minutes.

Phase 3 — Prove & prepare (Weeks 11–13)

- Collect evidence: logs, reviews, training attestations, supplier proofs, and test results.
- Run an internal audit/management review and finalize your NIS 2 status report.

Quick NIS 2 readiness checklist

- [ ] *Scope confirmed (sector, size-cap) and DORA carve-out assessed.*
- [ ] *ISMS workspace live; owners assigned per 13 domains.*
- [ ] *Policies approved by management; risk register and SoA in place.*
- [ ] *Incident pipeline (24/72/30) rehearsed; templates and contacts ready.*
- [ ] *Supplier list categorized; assurance and monitoring defined for critical vendors.*
- [ ] *Access control & MFA enforced for critical systems; backup/DR tested.*
- [ ] *Training rolled out to management and staff; evidence logging active.*
- [ ] *Internal audit/management review completed; gaps tracked to closure.*

Resources & next steps

Book a NIS 2 readiness review with Copla.

Use our ISO-to-NIS 2 control map to accelerate implementation.

Add the Vendor Register of Information and the contract clause pack to your procurement flow.

Copla