

Gap analysis from your security policy

Captured 2026-05-14T07:10:00Z · team tier · claude-opus-4-7

Scenario

Your CISO needs to know how today's information-security policy maps against ISO 27001, NIS2, and DORA — without buying three separate audits.

What was asked

What controls do ISO 27001:2022, NIS2 (Directive 2022/2555), and DORA (Regulation (EU) 2022/2554) each require from a regulated entity's information-security policy? Group by framework. Mark each requirement critical / material / minor with inline citations. (For a real gap analysis, attach your policy and the workflow will pair each control to your existing clause and flag the misses.)

Answer

Gap-analysis baseline — ISO 27001 + NIS2 + DORA

The gateway returned strong coverage on NIS2 and DORA (the two binding EU regimes) and thin coverage on ISO 27001 (the management-system standard). The control set below is the **superset of requirements** the three regimes impose on an in-scope entity. Pair each row against your existing policy clauses to produce a real gap analysis.

NIS2 — Directive (EU) 2022/2555

The gateway returned the following on-point NIS2 articles (and recitals giving their motivation):

- **Article 1 — Subject matter.** Establishes the harmonised cybersecurity-risk-management and reporting baseline across the Union.
- **Article 16 — Peer review framework.** Member-State authorities review each other; the operator-side impact is that supervisory expectations converge over time.
- **Article 20 — Governance.** Management bodies of essential and important entities **must approve the cybersecurity-risk-management measures** and oversee their implementation, can be held liable for non-compliance, and must follow specific training. **Critical.**
- **Article 21 — Cybersecurity risk-management measures.** This is the load-bearing article. Mandates **all-hazards** approach with at least: risk-analysis + information-system security policies; incident handling; business continuity (backups, disaster recovery, crisis management); supply-chain security; security in acquisition / development / maintenance; vulnerability disclosure; assessment of effectiveness; basic cyber-hygiene practices and training; cryptography use policy; HR security, access-control, asset management; MFA or continuous-authentication, secure voice/video/text comms; and emergency-comms systems. **Critical — every bullet is a policy clause.**

- **Article 32 — Supervisory and enforcement measures.** Competent authority has on-site inspection, ad-hoc audit, security scans, document requests, and can issue binding instructions. **Material — your policy must support evidentiary production within authority timeframes.**
- **Recitals 74, 78, 82, 85, 137** — explain risk-based proportionality, role of management bodies, supply-chain considerations.

DORA — Regulation (EU) 2022/2554

The gateway returned an equally strong DORA set:

- **Article 1 — Subject matter.** Uniform ICT-risk-management rules for financial entities.
- **Article 5 — Governance and organisation.** Management body owns ICT risk; defines and approves the ICT-risk-management framework; allocates the budget; sets the risk tolerance. **Critical.**
- **Article 6 — ICT risk-management framework.** Documented framework covering strategies, policies, procedures, tools necessary to address ICT risk. **Critical — the framework document IS the policy artifact.**
- **Article 13 — Learning and evolving.** Continuous learning from incidents and exercises; updates to the framework.
- **Article 16 — Simplified framework for small and non-interconnected entities.** Proportionality regime — confirm whether you qualify before assuming full Article 6 applies.
- **Article 24 — Testing.** ICT testing programme including vulnerability assessments, scans, source-code reviews, scenario-based tests, end-to-end tests at appropriate frequency.
- **Article 28 — Third-party-risk monitoring.** Register of ICT third-party providers; pre-contractual due diligence; ongoing monitoring; exit strategies. **Critical — supply chain is a frequent gap.**
- **Recitals 8, 43, 45** — proportionality, scope clarifications.

ISO 27001:2022

The gateway returned only **1 weakly-relevant result** from the ISO 27001 corpus for the search `information security management system requirements`. The on-point clauses (Clauses 4–10 of the standard plus Annex A controls) were not surfaced in this run, so the platform refuses to cite specific ISO 27001 clauses from training data. **For a real gap analysis against ISO 27001:2022 you'll want a more targeted query per clause** or a separate consultation against the standard text.

The binding requirements above (NIS2 + DORA) are mostly a superset of ISO 27001 Annex A anyway — an entity that implements them correctly will already satisfy the bulk of Annex A categories on access control, supplier relationships, incident management, cryptography, and continuity.

Bottom line

The NIS2 + DORA requirement set above gives you the gap-analysis backbone the gateway can ground today. To produce a real gap analysis, attach your information-security policy and the workflow will pair every clause against your existing language and flag the misses. A re-run targeted at ISO 27001 specific clauses can fill the third leg.

Tool calls

| # | Tool | Result |
|---|--------|---|
| 1 | search | 1 weakly-relevant result; ISO 27001 specific clauses not surfaced for this query |
| 2 | search | 10 results from EU Regulations MCP — NIS2 Art. 1, 16, 20, 21, 32 + Recitals 74, 78, 82, 85, 137 |
| 3 | search | 10 results from EU Regulations MCP — DORA Art. 1, 5, 6, 13, 16, 24, 28 + Recitals 8, 43, 45 |

Citations

| Type | Jurisdiction | Reference | URL |
|------------|--------------|--|---|
| regulation | EU | NIS2 Directive (EU) 2022/2555 Article 1 — Subject matter | https://eur-lex.europa.eu/eli/dir/2022/2555/oj |
| regulation | EU | NIS2 Article 20 — Governance | https://eur-lex.europa.eu/eli/dir/2022/2555/oj |
| regulation | EU | NIS2 Article 21 — Cybersecurity risk-management measures | https://eur-lex.europa.eu/eli/dir/2022/2555/oj |
| regulation | EU | NIS2 Article 32 — Supervisory and enforcement measures | https://eur-lex.europa.eu/eli/dir/2022/2555/oj |
| regulation | EU | DORA Regulation (EU) 2022/2554 Article 5 — Governance and organisation | https://eur-lex.europa.eu/eli/reg/2022/2554/oj |
| regulation | EU | DORA Article 6 — ICT risk-management framework | https://eur-lex.europa.eu/eli/reg/2022/2554/oj |
| regulation | EU | DORA Article 13 — Learning and evolving | https://eur-lex.europa.eu/eli/reg/2022/2554/oj |
| regulation | EU | DORA Article 16 — Simplified framework | https://eur-lex.europa.eu/eli/reg/2022/2554/oj |
| regulation | EU | DORA Article 24 — Testing of ICT tools and systems | https://eur-lex.europa.eu/eli/reg/2022/2554/oj |
| regulation | EU | DORA Article 28 — Third-party-risk monitoring | https://eur-lex.europa.eu/eli/reg/2022/2554/oj |

Generated by Ansvar AI Gateway. This is the same artifact a customer would receive.

<https://gateway.ansvar.eu> · 2026-05-14T07:10:00Z