ÆNIX

NIS2 Compliance Readiness Checklist

35 architectural control points to assess whether your cloud platform supports the cybersecurity risk-management measures required by Directive (EU) 2022/2555.

For CISOs, security & compliance leads · aenix.io

35 architectural control points for essential and important entities. Aligned to Directive (EU) 2022/2555.
Member State transposition deadline 17 October 2024. v1.1 — September 2026.

How to use this checklist

The Network and Information Security 2 Directive (NIS2, Directive (EU) 2022/2555) significantly expands the scope and rigour of EU cybersecurity obligations. Member States transposed it into national law on 17 October 2024 (with some still finalising sectoral implementation). NIS2 covers essential entities (energy, transport, banking, financial market infrastructure, healthcare, drinking water, wastewater, digital infrastructure, ICT-service management, public administration, space) and important entities (postal, waste, manufacture of critical products, food distribution, manufacture of certain digital services, R&D).

This 35-point checklist gives CISOs, compliance leads, and platform engineering managers a structured way to assess whether their architecture supports the cybersecurity risk-management measures required under Art. 21 Art. 23 and adjacent provisions.

Use it in three ways:

1. **Self-assessment** — walk through with security, platform engineering, and compliance teams.
2. **Authority dialog preparation** — section summaries map directly to a control narrative for a national CSIRT or competent authority.
3. **Supplier scoping** — share with ICT third parties (especially ICT-service-management providers) so they answer against the same surface.

> This checklist is an architectural readiness aid, not legal advice. NIS2 conformance must be confirmed by your legal counsel and validated against the national transposition in each Member State where you are in scope. Sectoral lex-specialis (DORA for financial entities, eIDAS for trust services) may take precedence in specific areas.

Section coverage:

SECTION	FOCUS	POINTS
1	Risk management Art. 21	10
2	Incident handling & reporting Art. 23	6
3	Business continuity & vulnerability management	7
4	Supply chain & cryptography	6
5	Access control & audit	6

1. Risk management Art. 21

Article 21 enumerates the cybersecurity risk-management measures essential and important entities must implement. These are structural controls — designed to be evidenced, not just claimed.

- [ ] **Risk register documented per critical workload** — inventoried, owned, reviewed. Art. 21(2)(a)
- [ ] **Annual cybersecurity risk review** — conducted and signed by the management body. Art. 21(2)(a)
- [ ] **ICT asset register complete and current** — all hardware, software, data, and dependencies tracked. Art. 21(2)(i)
- [ ] **Threat model documented per critical workload** — updated on material architectural change. Art. 21(2)(a)
- [ ] **Cybersecurity policy approved by management body** — documented, refreshed annually. Art. 20
- [ ] **Network segmentation / zero-trust enforcement** — microsegmentation between trust zones; default-deny posture. Art. 21(2)(a)
- [ ] **Pod Security Standards / NetworkPolicies enforced (Kubernetes)** — where Kubernetes is in use, or equivalent isolation primitives on other substrates. Art. 21(2)(a)
- [ ] **Effectiveness review of controls — quarterly** — documented evidence retained. Art. 21(2)(f)
- [ ] **Cybersecurity training mandatory for all staff** — including senior management; completion tracked. Art. 21(2)(g) Art. 20
- [ ] **Risk register reviewed by audit annually** — internal or external audit; findings tracked to remediation. Art. 21(2)(f)

> Article 20 places direct accountability on management bodies for approving cybersecurity measures and overseeing their implementation. "Risk owned by IT" is no longer a defensible posture.

2. Incident handling & reporting Art. 23

NIS2 introduces tight reporting timelines — early warning within 24 hours, incident notification within 72 hours, and a final report within 1 month.

- [ ] **24×7 detection capability for critical workloads** — aligned to the severity classification used for reporting. Art. 23
- [ ] **Documented incident response with named roles** — IR plan with on-call, escalation paths, decision authority, and comms playbook.
- [ ] **Incident classification process documented** — "significant" vs non-significant thresholds explicitly defined.
- [ ] **Pre-established CSIRT / competent-authority communication channels** — named contacts, secure channels, mock exercise completed.
- [ ] **Reporting templates aligned to 24-hour / 72-hour / 1-month** — templates tested, owners assigned. Art. 23(4)
- [ ] **Annual incident-response exercise** — tabletop or live; results retained.

> The 24-hour early warning is intentionally short — it requires a process where on-call security can make a "report or not" decision very quickly. Build the decision rubric into the IR plan, not into the incident.

3. Business continuity & vulnerability management

- [ ] **BCP plan per critical workload** — documented, owned, reviewed. Art. 21(2)(c)
- [ ] **RTO / RPO documented and tested annually** — with evidence of test, not just a plan. Art. 21(2)(c)
- [ ] **Backup recovery tested in the past 12 months** — successful restore from a production backup to a clean environment.
- [ ] **DR site operational and tested** — failover exercised within the last 12 months for critical workloads.
- [ ] **CVE response SLA documented** — triage / patch / verification windows by severity. Art. 21(2)(e)
- [ ] **SAST / DAST in CI; container scanning + SBOM** — build-time security gates; dependency provenance tracked.
- [ ] **Coordinated vulnerability disclosure policy published** — receipt channel, triage commitment, recognition. Art. 12

> For container workloads, "SBOM" should mean a generated, signed, retained artifact (e.g. SPDX or CycloneDX format) — not a manual spreadsheet. Use Sigstore / Cosign or an equivalent for signatures.

4. Supply chain & cryptography

NIS2 places explicit weight on supply-chain risk Art. 21(2)(d) and on cryptography and encryption Art. 21(2)(h).

- [ ] **ICT third-party inventory complete** — all ICT providers, including indirect (sub-contracted). Art. 21(2)(d)
- [ ] **Critical-function dependencies mapped to the second hop** — sub-contractors of suppliers, where they perform critical functions.
- [ ] **Article 21(2)(d)-aligned contractual content in critical-function agreements** — including coordinated vulnerability disclosure provisions and incident communication. Art. 21(2)(d)
- [ ] **Continuous supplier monitoring documented** — annual review minimum; ad-hoc on incident or M&A trigger.
- [ ] **Encryption at-rest, in-transit, and (where applicable) in-use** — with documented cipher choices and rotation. Art. 21(2)(h)
- [ ] **Customer-controlled encryption keys where applicable** — for tier-1 / sensitive workloads. Key-custody process documented.

> "Supply chain to the second hop" sounds onerous but is largely about knowing, not controlling. The register often surfaces concentration on the same underlying provider via different intermediaries — useful intelligence regardless of the NIS2 framing.

5. Access control & audit

NIS2 expects MFA, privileged access management, and audit completeness as baseline controls — not advanced ones.

- [ ] **MFA for privileged accounts (universal)** — all admin / break-glass / IAM accounts; no exceptions. Art. 21(2)(j)
- [ ] **MFA for end-user access where reasonable** — risk-based for non-privileged access.
- [ ] **Privileged access management deployed** — just-in-time elevation, session recording, vault for shared credentials.
- [ ] **Joiner-mover-leaver automated** — identity lifecycle from the HR system to all in-scope systems; access removal verified.
- [ ] **Audit log retention meets the longest applicable requirement** — often 5+ years for sectoral or national mandates; tamper-evident storage.
- [ ] **Authority access process documented and tested** — procedure for granting a national CSIRT or competent authority access; mock exercise completed.

> Many organisations have MFA on the SSO surface but missing on cloud-provider root accounts, third-party SaaS admin consoles, or legacy break-glass paths. Audit comprehensively — not just the front door.

Architecture-level recommendations

For most NIS2 controls, architecture is the most leveraged remediation surface. Where the underlying platform structurally supports tenant isolation, customer-controlled encryption, an immutable audit trail, controlled supplier access, and tested exit/restore mechanics, many of the 35 checkpoints become consequences of design rather than separate compliance projects.

When architecture closes NIS2 gaps structurally

- Tenant CRD multi-tenancy addresses Art. 21(2)(a) network segmentation and isolation between trust zones.
- Customer-controlled encryption at platform, storage, and observability layers addresses Art. 21(2)(h).
- Air-gap support addresses sovereign / regulator-isolated workload requirements where national law goes beyond the NIS2 baseline.
- Audit-trail completeness (provider-side via VictoriaLogs, customer-side via export) addresses Art. 21(2)(i) and authority-access expectations.
- Tested exit and restore mechanics address Art. 21(2)(c) BCP and the supplier-exit expectations of Art. 21(2)(d).

When existing architecture can be retrofitted

- Many controls (universal MFA, CVE SLA, CVD policy, training, risk-register cadence, JML automation) are organisational and tooling additions that do not require platform replacement.
- Network segmentation and microsegmentation can usually be retrofitted on Kubernetes-based platforms via NetworkPolicy / Cilium policy without an architectural rebuild.
- BCP / DR and backup-test cadence is process discipline — no platform change needed.

When a partial retrofit is genuinely insufficient

- VMware-Cloud-Director-based platforms struggle with portability (Art. 21(2)(d) supplier exit) and customer-controlled keys at every layer.
- Vendor-managed-only encryption, especially for backups and observability, fails Art. 21(2)(h) where regulator scrutiny is high.
- Multi-tenant SaaS shared infrastructure struggles with audit-trail completeness expectations under authority scrutiny.

> The most cost-effective gap-closure sequence is usually: (1) universal MFA + JML, (2) backup test + DR test, (3) CVE SLA + SBOM, (4) supplier register + contracting refresh, (5) architectural changes if and where steps 1–4 cannot close the gap.

NIS2-aligned cloud architecture — reference pattern

A platform built around isolation, customer-controlled cryptography, and immutable auditability can close most Article 21 controls at the platform layer rather than as 35 compensating procedures. The reference pattern below stacks three layers.

Tenant plane

Isolated tenants side by side — for example a production tenant, an audit-isolated tenant, a sovereign-workloads tenant, and a test tenant. Each carries its own encryption keys, audit-log stream, and MFA-gated access.

Platform control plane

A single Kubernetes-native control plane providing the Tenant CRD, identity (OIDC), NetworkPolicy / Cilium segmentation, encryption (BYOK / HYOK), an audit pipeline (VictoriaLogs to an immutable backend), and backup orchestration.

Substrate

In-region datacenter, an in-region DR site, and an optional air-gapped enclave for regulator-isolated workloads.

ARCHITECTURE ELEMENT	NIS2 CONTROL AREA
Per-tenant encryption keys	Art. 21(2)(h) Customer-controlled encryption
NetworkPolicy / Cilium	Art. 21(2)(a) Segmentation
Audit pipeline	Art. 21(2)(i) Art. 23
Multi-datacenter + DR site	Art. 21(2)(c) Continuity & DR
MFA-gated tenant access	Art. 21(2)(j) Access control
Tenant CRD isolation	Art. 21(2)(d) Supplier exit / portability

This pattern is not the only valid NIS2-aligned architecture — but it illustrates how isolation, customer-controlled cryptography, and immutable auditability close most Article 21 controls at the platform layer.

Next steps

Option 1 — Self-remediate using this checklist. Walk through it with security, platform, and compliance teams. Convert unchecked boxes into a 90-day remediation plan.

Option 2 — NIS2-aligned readiness engagement with Aenix (4–6 weeks). We run the checklist with you, review architecture against each control, and produce a remediation plan with effort estimates and authority-narrative drafts. Fixed-fee engagement.

Option 3 — Joint NIS2 + DORA + GDPR mapping. For entities in scope of multiple frameworks. We map controls to avoid duplicated work and surface where one framework satisfies several.

Schedule a discovery call: aenix.io/services/platform-readiness-assessment/

Refresh cadence

- **Quarterly:** review against new national transpositions and supervisory communications.
- **Annual:** structural review of checklist coverage.
- **Ad-hoc:** on material amendments to NIS2 itself or to sectoral lex-specialis.

Aenix is the team behind Cozystack (a CNCF project) and offers the Ænix Platform — our commercial productized offering based on Cozystack. aenix.io

Aenix · aenix.io · NIS2 Compliance Readiness Checklist · v1.1 — September 2026. Aenix is the team behind Cozystack (CNCF, Apache 2.0).