TARA INNOVA

NIS2 Compliance Guide

How TARA INNOVA Maps to NIS2 Directive Requirements

What Is NIS2

The NIS2 Directive (EU 2022/2555) is the European Union's updated framework for cybersecurity across essential and important entities. It entered into force in January 2023 with member state transposition deadlines from October 2024. NIS2 significantly expands scope, strengthens requirements, and introduces personal liability for management bodies.

Who Is Affected

NIS2 applies to essential entities (energy, transport, banking, health, water, digital infrastructure, public administration, space) and important entities (postal services, waste management, chemicals, food, manufacturing, digital providers, research). Organizations with 50+ employees or €10M+ turnover in these sectors fall within scope.

Key Requirements and TARA INNOVA Coverage

NIS2 Requirement	TARA INNOVA Coverage
Art. 21(2)(a) — Risk analysis and information system security policies	CRP generates continuous risk posture reports. Quicksand enforces security policies at the edge with full audit trail.
Art. 21(2)(b) — Incident handling	Quicksand detects and blocks threats in real time. CRP auto-generates incident reports with timelines, classification, and remediation records.
Art. 21(2)(c) — Business continuity and crisis management	Multi-deployment architecture (on-prem, hybrid, cloud) ensures enforcement continuity. CRP documents recovery procedures and control effectiveness.
Art. 21(2)(d) — Supply chain security	Quicksand validates third-party traffic. TI Cloud provides threat intelligence on supplier-related indicators. CRP maps evidence to supply chain controls.
Art. 21(2)(e) — Security in network and information systems	Quicksand provides L4/L7 traffic inspection, rate limiting, and geo-enforcement. Oasis secures IoT/OT integration channels.
Art. 21(2)(g) — Cybersecurity training and hygiene	CRP tracks training completion and security awareness metrics. Role-based access ensures least privilege across the platform.
Art. 21(2)(j) — Multi-factor authentication and encryption	Quicksand enforces session integrity with PoW challenges and device trust verification. mTLS for all service-to-service communication.
Art. 23 — Incident notification (24h/72h/1mo)	CRP generates pre-formatted notification packages within regulatory timelines. Evidence packages assembled automatically from enforcement data.

Continuous Compliance, Not Point-in-Time

NIS2 requires entities to demonstrate ongoing compliance — not just pass an annual audit. The TARA INNOVA platform generates evidence continuously from operational enforcement data. When auditors or regulators arrive, documentation is already assembled.

- **Automatic evidence capture** — Every enforcement decision becomes a compliance record
- **Framework-mapped reports** — Evidence linked to specific NIS2 articles and annexes
- **Incident timeline reconstruction** — Full causal chain from detection to remediation
- **Management body reporting** — Board-ready summaries demonstrating due diligence (Art. 20 liability)

Deployment for NIS2 Compliance

TARA INNOVA deploys entirely within your infrastructure — on-premise, hybrid, or private cloud. No data leaves your environment. EU-headquartered with no third-country data transfers. This directly addresses NIS2's emphasis on data sovereignty and jurisdictional control.