TARA
INNOVA

DORA Compliance Guide

How TARA INNOVA Maps to the Digital Operational Resilience Act

What Is DORA

The Digital Operational Resilience Act (EU 2022/2554) establishes a unified ICT risk management framework for the European financial sector. Applicable from January 2025, DORA requires financial entities to manage, test, and report on their digital operational resilience — with specific obligations around ICT risk management, incident handling, resilience testing, and third-party risk.

Who Is Affected

DORA applies to credit institutions, investment firms, insurance undertakings, payment institutions, crypto-asset service providers, central securities depositories, trading venues, and their critical ICT third-party service providers. Nearly all regulated financial entities in the EU are in scope.

Key Requirements and TARA INNOVA Coverage

DORA Requirement	TARA INNOVA Coverage
Art. 6–16 — ICT risk management framework	Quicksand enforces risk-based traffic policies. CRP continuously documents control effectiveness and risk posture changes.
Art. 17–23 — ICT-related incident management	Real-time detection and blocking via Quicksand. CRP generates incident classification, impact assessment, and notification packages within DORA timelines.
Art. 24–27 — Digital operational resilience testing	Multi-deployment architecture supports resilience testing. CRP documents test scenarios, results, and remediation tracking.
Art. 28–44 — Third-party ICT risk management	TI Cloud monitors threat indicators related to third-party services. Quicksand enforces boundary controls on third-party traffic. CRP maps evidence to vendor risk assessments.
Art. 45–56 — Information sharing	TI Cloud enables privacy-preserving threat intelligence sharing with industry peers, ISACs, and CERTs — without exposing internal infrastructure.

ICT Incident Reporting Under DORA

DORA mandates structured incident reporting with specific timelines and content requirements. The Compliance Report Portal automates this process:

Report	Timeline / Content
Initial notification	Within 4 hours of classification. CRP auto-generates with incident type, impact scope, and affected services.
Intermediate report	Within 72 hours. CRP compiles response timeline, root cause analysis progress, and containment measures.
Final report	Within 1 month. Full incident report with timeline, causal analysis, remediation actions, and lessons learned.

Continuous Evidence for Financial Regulators

- **Immutable audit trail** — Every enforcement decision recorded with tamper-evident integrity
- **Regulator-ready packages** — Pre-formatted for ECB, BaFin, ACPR, DNB, and national competent authorities
- **Control effectiveness metrics** — Quantified protection rates, response times, and gap analysis
- **Board accountability** — Executive summaries mapping security posture to DORA obligations
- **Third-party risk documentation** — Evidence of boundary controls and monitoring for ICT service providers

Deployment for Financial Sector

TARA INNOVA deploys on-premise or in your private cloud — critical for financial entities with strict data residency requirements. EU-headquartered with no third-country data transfers. Multi-tenant isolation supports group-level deployment across subsidiaries with entity-specific evidence and reporting.