Ropo

DORA Adoption Policy

Voluntary application of the EU Digital Operational Resilience Act as a reference framework

June 2026
Kuopio, Finland

1. Purpose and scope

DORA (Regulation (EU) 2022/2554) does not apply to Ropo as a binding obligation. Ropo is not a credit institution, a payment institution, an electronic money institution, or any other financial entity listed in Article 2, and it is not an ICT third-party service provider in the sense DORA defines.

Ropo provides invoice lifecycle services, including debt collection, across the Nordic region — principally Finland, Sweden, and Norway — and in doing so handles client funds each year.

Its statutory ICT and cybersecurity obligations arise under NIS2 and its national transpositions, together with GDPR. Its debt-collection activity is supervised under the national debt-collection regime applicable in each market.

Ropo adopts DORA as a reference framework within its ISMS by choice. At this transaction volume, operational resilience is a material exposure whether or not any regulation compels it.

Many of Ropo's clients are themselves bound by DORA and must manage Ropo as a service provider under their own obligations. Applying DORA's principles proportionately lets Ropo meet that demand through a single control set rather than a separate compliance track.

This adoption rests on Ropo's position that it is not a payment institution. Should that determination change, DORA could apply directly, and this policy would be reissued on a mandatory basis.

The policy covers the systems, services, processes, and suppliers that support Ropo's services across the group.

2. Relationship to binding obligations

Ropo's binding ICT and cybersecurity obligations sit under NIS2 and its national transpositions in the countries where Ropo operates. Where an incident meets the reporting threshold, Ropo notifies affected clients and reports to the relevant national authority — the national cyber security centre or CSIRT in the country concerned — within the applicable timelines.

Personal data is governed by GDPR and its breach-notification rules.

DORA sits alongside these as an adopted framework, not a legal requirement. Where this policy refers to DORA, it means DORA's principles applied in proportion to Ropo's role — not compliance with obligations owed to a financial supervisor.

Ropo does not file DORA incident reports with any financial supervisory authority, does not submit the ESA register of information, and is not subject to DORA's testing or oversight regimes.

All three frameworks are managed through one ISMS aligned to ISO/IEC 27001, so that controls are defined and evidenced once rather than maintained in parallel.

3. Governance and accountability

3.1 Management oversight

Top management is accountable for operational resilience and for providing the resources and structures it requires. Governance runs through the Security Council, which owns risk management and control effectiveness across the group.
The CIO, the Security Council, and the Group Management Team track resilience through defined metrics, internal audits, and management reviews.

3.2 ICT risk management framework

ICT risks are managed through a risk-based framework within the ISMS, aligned to ISO/IEC 27001, with risks mapped to implemented controls. The framework identifies Ropo's critical functions, including invoicing, payment handling, debt collection, and customer service.
The systems and suppliers supporting those functions are identified so that protection and monitoring are concentrated where disruption would matter most. A named owner within the Security function is responsible for oversight of ICT third-party arrangements.
Risk assessments are revised when systems, suppliers, or threats change, and after incidents and audits.

4. ICT security and operational resilience controls

4.1 Technical and organisational measures

The controls that protect Ropo's services are defined in the ISMS and its Statement of Applicability. These include access control, identity management, logging, monitoring, vulnerability management, and encryption.
The controls are reviewed through monitoring, testing, and audit, and adjusted as threats change. This policy does not restate them; the ISMS is the source of record.

4.2 Incident management and reporting

A single incident process governs detection, classification, escalation, and resolution across the organisation.
Reporting follows Ropo's binding obligations under NIS2. Where an incident affects a client's service or data, Ropo notifies the client without undue delay.

Where the NIS2 threshold is met, Ropo reports to the relevant national authority in the affected country within the required timelines. For clients that are themselves bound by DORA, Ropo provides the incident information they need to meet their own reporting obligations.
Ropo has no statutory reporting line to any financial supervisory authority. In the limited case where an incident materially impairs a supervised client's ability to meet its own obligations, Ropo may escalate to the relevant financial supervisor as a discretionary courtesy.
This is not a compliance obligation and does not replace the client's own reporting.
Incidents are reviewed after resolution, and the findings feed back into controls, training, and processes.

4.3 Resilience testing

Resilience is tested through vulnerability scanning, penetration testing, and operational monitoring. These activities are supported by disaster-recovery and business-continuity exercises with defined recovery time and recovery point objectives.
Backups are held separately from production so that they survive an incident affecting primary systems.
Findings are assigned to owners and tracked to closure, and they drive changes to architecture and controls.
Threat-led penetration testing under DORA Article 26 applies to significant financial entities and does not apply to Ropo. Testing is scaled to Ropo's own risk profile.

5. Third-party risk and ICT service providers

Third-party risk is managed through Ropo's supplier lifecycle. Ropo maintains an internal register of its ICT suppliers and the services they support, classified by criticality.
This is Ropo's own inventory, not the ESA register of information, which Ropo is not required to submit.
Suppliers are subject to due diligence before engagement and to monitoring throughout the relationship.
Contracts set requirements for ICT security, incident notification, audit rights, service continuity, data ownership, data protection, and exit.
For suppliers that support a critical function, Ropo maintains an exit strategy and assesses concentration risk, so that the failure or loss of a single provider does not by itself threaten service continuity.
Changes that affect risk, including a new sub-processor or a service disruption, are assessed as they arise.

6. Roles and responsibilities

Top management sets direction and provides oversight. The CIO and the Security Council guide implementation, monitor performance, and approve improvements.

The Security and Compliance functions run the ICT risk framework, coordinate testing, operate the incident process, and oversee supplier risk. Legal handles regulatory and contractual alignment. Business and IT teams implement controls, maintain systems, and keep services running.

7. Review and continuous improvement

The policy is reviewed at least once a year, and sooner if a material change in Ropo's activities, risk profile, or regulatory position warrants it. The CIO drives the review and governance approves it, on the basis of evidence from audits, incidents, testing, and risk assessments.
Findings from monitoring and incidents drive corrective action across people, processes, and technology. Corrective actions are managed through the ISMS.