

**Report: DORA**

**Loft Company DORA + Core Questions + Audit + In Depth**

v1.0.2026-04-15

Created: 2026-04-15 10:30

Closed: 2026-04-15 10:45

Answered: 97%

Compliance Score:

**96%**

(239/248)

**|** Almost all requirements met; very low risk.

A very little uncertainty due to small fraction of measuring points not addressed.

---

**Top Risks:**

**Risk Management – 25% Compliant**

1. Are responsibilities for ICT risk management clearly defined and assigned? Unanswered

Criticality: High

**Risk Management – 25% Compliant**

2. Is there a documented ICT risk management framework in place? Partially

Criticality: High

---

### Compliance By Section:

Risk Management	85%	ICTSecurity	100%	Incident Reporting	100%
Third Party Providers	100%	Testing	100%		

### Compliance by Criticality

Criticality	Measurement Points	Yes	Partially	No	Missing	Compliance %
Critical	1	1	0	0	0	100 %
High	31	29	1	0	1	95 %
Medium	13	13	0	0	0	100 %
<b>Total</b>	<b>45</b>	<b>43</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>96 %</b>

## ICTSecurity

*Covers technical and organisational measures to ensure ICT systems and data are secure, resilient, and monitored.*

Are access rights to ICT systems based on least privilege principles? **Yes**

Criticality: High

Is sensitive data protected with encryption in transit and at rest? **Yes**

Criticality: High

Are ICT systems monitored for security events and anomalies? **Yes**

Criticality: High

**<< The rest of this section is left out in this sample/preview >>**

---

## Recommendations:

### Risk Management

*Covers the organization's ICT risk management framework, governance, and operational resilience planning.*

**1. Implement and document an ICT risk management framework covering identification, assessment, and mitigation of risks.**

Criticality: High

**2. Clearly define and assign responsibilities for ICT risk management across relevant roles.**

Criticality: High

---

---

Compliance Score: 96% (239/248)

Almost all requirements met; very low risk.