DORA: what it requires, what is at stake, and who is accountable

For management-body members of EU-licensed financial entities (EMIs, Payment Institutions, CASPs). One page. No jargon.

THE FIVE DORA PILLARS — WHAT SUPERVISORS EXAMINE

PILLAR 01

ICT Risk Management

Documented framework, asset classification, risk assessments, named ownership. Evidence of regular review by the management body.

PILLAR 02

ICT Incident Reporting

Classification criteria (major vs minor). Playbooks with 4-hour, 24-hour, 72-hour, and 1-month reporting to the national competent authority.

PILLAR 03

Resilience Testing

Annual testing programme (vulnerability scans, pen tests, DR drills). Threat-Led Penetration Testing (TLPT) every 3 years for designated entities.

PILLAR 04

Third-Party ICT Risk

Register of Information (full supplier map in NCA format). DORA-compliant contract clauses. Concentration risk analysis. Exit strategies.

PILLAR 05

Information Sharing & Reporting

Participation in threat intelligence sharing arrangements. Regular internal ICT risk reporting to the management body. Board oversight documented and traceable.

SUPERVISORY TIMELINE — WHERE 2026 SITS

Jan 2025
DORA applied. All obligations in force for in-scope financial entities.

2026 — now
Active supervisory phase. Regulators are issuing information requests and requesting operating evidence — not just policy existence.

2027+
TLPT cycle and ongoing supervisory reviews. Evidence gaps from 2025–26 become a supervisory record.

MANAGEMENT-BODY ACCOUNTABILITY — THE PERSONAL EXPOSURE

Under DORA (Articles 50–52) and national NIS2 transpositions (Articles 32–33), cybersecurity governance is not a technical matter delegated to IT. It is a **management-body obligation**. Supervisors may apply personal measures to individual decision-makers where national law allows — including temporary bans from management functions.

DORA — legal entity
Up to 1% of average daily worldwide turnover, applied per day for up to 6 months (Art. 50)

NIS2 — essential entities
Up to €10M or 2% of global annual turnover (Art. 34)

NIS2 — important entities
Up to €7M or 1.4% of global annual turnover (Art. 34)

Your options — and what each one actually costs

For management-body sign-off. Honest comparison across the realistic alternatives. Does not include doing nothing (exposure is open-ended).

CRITERIA	CYADVISO VCISO	FULL-TIME CISO	BIG 4 / LAW FIRM	GRC PLATFORM	COMPLIANCE OFFICER COVERS IT
Annual cost	€36–60K	€150–260K+	€80–200K	€5–15K	€0 incremental
DORA expertise	Deep	Depends	Legal yes; technical gaps	SOC2/ISO27001 only; DORA gaps	Wrong domain
Technical implementation	Full	Full	Advisory only	Self-service	Out of scope
Board reporting	Included	Included	Extra cost	No	Legal flavour only
Time to audit-ready	90 days	3–6 months after hire	3–12 months	Depends on team	Indefinite
Named ICT-risk owner	Yes — from day 1	Yes	No	No	No
Regulator exposure	Managed	Managed	Partial	Partial	False confidence

ILLUSTRATIVE COST OF INACTION — ON €10M ANNUAL REVENUE

Reference: DORA Art. 50 daily fine schedule	
DORA daily fine (1% of daily turnover)	**~€274 / day**
6 months of daily fines — maximum under Art. 50	**~€50,000**
Management-body personal measures (Art. 52)	**unquantifiable**
Quarter without named ICT-risk ownership	**90 days of exposure**
CyAdviso 12-month retainer (closes the gap)	**€36–60K**

NEXT STEP

Andrey Gubarev
vCISO · Founder, SIA CyAdviso

CISM · CDPSE · SABSA · Based in Riga, Latvia, EU

Email: info@cyadviso.com
Phone: +371 2716 6168
Book a 15-min call: cyadviso.com
LinkedIn: linkedin.com/in/andreygubarev

15-minute scoping call. Walk away with a clear gap picture and a cost we can scope. No commitment.