DORA BOARD BRIEFING

What must be *owned*, evidenced and funded — by 2026.

A two-page management-body summary for EU-licensed fintechs — EMIs, payment institutions, CASPs, investment firms and other DORA in-scope financial entities. Read once. Decide. Move.

PILLARS IN SCOPE	IN FORCE SINCE	SUPERVISOR EXPECTATION
5 ICT risk · Incidents · Testing · 3rd parties · Governance	17 Jan 2025	Operating evidence, not policy text

§ 01 WHAT DORA REQUIRES SUPERVISORS TO SEE

PILLAR 01	PILLAR 02	PILLAR 03	PILLAR 04	PILLAR 05
ICT risk management	**Incident reporting**	**Resilience testing**	**ICT third parties**	**Governance evidence**
Named ownership, asset classification, risk acceptance, controls and board review.	Major-incident classification, escalation, NCA filing route and post-incident record.	Annual ICT testing, DR evidence, remediation tracking and TLPT where designated.	Register of Information, contract clauses, concentration risk and exit plans.	Management-body reporting, decisions, exceptions and evidence of active oversight.

§ 02 WHERE 2026 SITS

17 Jan 2025

DORA started to apply. Readiness is no longer a future-state project.

2026 — now

Supervisors ask for operating evidence: records, registers and decisions.

2027 +

Evidence gaps become supervisory history — not just project backlog.

§ 03 THE BOARD QUESTION

> *The management body should not ask only* **"are we compliant?"** *— the practical question is: can we show* **who owns ICT risk, what was tested,** *what failed, what was fixed, and what was reported?*

§ 04 PERSONAL EXPOSURE

- DORA makes the **management body responsible** for approving, overseeing and being accountable for the ICT risk management framework.
- Administrative penalties and remedial measures are set by Member-State law; where national law allows, they can apply to **management-body members and responsible individuals**.
- NIS2 may add personal-management consequences under national transposition, including **temporary management-function restrictions** for essential entities.

The highest practical exposure is often **not a fine**. *It is a documented failure to supervise, fund and evidence remediation after warnings or incidents.*

§ 05 EVIDENCE THE BOARD SHOULD REQUEST

QUESTION	EXPECTED EVIDENCE
Who owns ICT risk?	Named owner, RACI, board reporting line.
Can we report a major incident?	Classification matrix, NCA route, tested playbook.
Which providers are critical?	Register of Information and concentration view.
What has been tested?	Annual test plan, DR records, remediation log.
What remains unfunded?	Risk-acceptance paper with dates and owners.

DECISION PAGE

What a credible solution costs — and *what decision is needed.*

The board does not need a tool decision first. It needs an **ownership decision**, a **funding envelope**, and a **date** when evidence must be audit-ready.

§ 06 REALISTIC IMPLEMENTATION OPTIONS

RECOMMENDED

vCISO / DORA operating model

€36–60K / year

Best when the entity needs named ownership, evidence and board reporting — quickly.

+ 90-day evidence roadmap
+ ICT-risk owner from day one
+ Register, incident process, board pack
+ Works for lean fintech teams

Full-time CISO hire

€150–260K+ / year

Best when the company has scale and time to recruit, onboard and retain senior talent.

+ Strong long-term model
– 3–6 months hiring lead time
– Still needs implementation budget
– Overkill for many fintech SMBs

GRC platform or legal review

€5–200K

Useful support — but not a substitute for operating ownership and evidence creation.

+ Can structure documents
– Does not run ICT risk
– May miss technical implementation
– Risk of false confidence

§ 07 BOARD DECISION CHECKLIST

- [ ] Confirm the **accountable management-body sponsor**.
- [ ] Approve the ICT-risk ownership model: **internal, vCISO or full-time hire**.
- [ ] Approve a **90-day evidence remediation plan** with named owners.
- [ ] Require **monthly reporting** until Register, incident process and testing records are audit-ready.
- [ ] Record any unfunded risk explicitly — **owner, expiry date, reopening trigger**.

§ 08 WHAT "AUDIT-READY" SHOULD MEAN

AREA	MINIMUM BOARD-READY OUTPUT
Governance	Board-approved ICT-risk framework and reporting cadence.
Incidents	Major-incident playbook with NCA route and escalation owners.
Third parties	Register of Information, critical functions, exit view.
Testing	Annual test plan, DR evidence, remediation tracker.
Oversight	Management-body pack: decisions, gaps, dates.

RECOMMENDED RESOLUTION

Approve a **90-day DORA evidence programme**, appoint an **accountable ICT-risk owner**, and require a management-body update **every month** until the entity can show operating evidence across incident reporting, third-party ICT risk, resilience testing and board oversight.

CYADVISO · NEXT STEP

15-minute scoping call with Andrey Gubarev

vCISO and founder of SIA CyAdviso. CISM · CDPSE · SABSA. Fintech cybersecurity, ICT risk and DORA operating evidence.

cyadviso.com
info@cyadviso.com
+371 2716 6168
linkedin.com/in/andreygubarev

Based on DORA Articles 5, 19, 25, 26, 28, 30, 50–52 and NIS2 Articles 20, 21, 32–34. Not legal advice.