gart.

WHITEPAPER

DORA Operational Resilience & Compliance

A practical guide of Moving EU financial organizations from "Are we compliant?" to "Are we actually ready?"

Prepared by :

Gart Solutions

Issued :

September 2026

gartsolutions.com

info@gartsolutions.com

Intro

Compliance is not the same thing as resilience.

The Digital Operational Resilience Act (DORA) became directly applicable across **the EU on 17 January 2025**, and 2026 is the year enforcement stops being theoretical.

Regulators have moved from accepting good-faith documentation to testing whether ICT risk frameworks actually hold up under pressure — automated cross-checks of ICT registers, the first wave of direct oversight of critical ICT third-party providers, and real financial and personal penalties for gaps that used to be tolerated as “work in progress.”

We see one challenge again and again when financial organizations start preparing for DORA: it cannot be solved by lawyers alone, and it cannot be solved by IT policies alone.

DORA sits exactly at the intersection of regulation, technology, cybersecurity, and business operations — which means a binder of policies with no operational backbone, or a security stack with no governance behind it, both fail the same test.

This whitepaper walks through **what DORA actually requires, what changed in 2026, where organizations most often get stuck, and how Gart Solutions' DORA Operational Resilience & Compliance service helps you build a system** where regulatory requirements are directly connected to the technology and operational processes that keep the business running — not just another folder of policies.

21	5	2%
categories of EU financial entities in scope	core pillars of the regulation	of annual global turnover — maximum entity-level fine

Why DORA, why now

DORA (Regulation (EU) 2022/2554) entered into force in January 2023 and became directly applicable on 17 January 2025, harmonizing ICT risk management across the EU financial sector for the first time. It replaces a patchwork of national and sector-specific rules with one binding framework covering roughly 21 categories of financial entities — banks, payment and e-money institutions, investment firms, trading venues, insurers and reinsurers, fund managers, crypto-asset service providers, crowdfunding platforms — and, critically, the ICT third parties they depend on.

2026: the grace period is over
In its first year, supervisors largely accepted documented intent — a policy on paper, a register in progress. That tolerance is gone.

Through 2026, national competent authorities and the European Supervisory Authorities (EBA, ESMA, EIOPA) have shifted toward testing operational effectiveness, not just paperwork:

- **Direct oversight has begun.** In November 2025 the ESAs published the first list of Critical ICT Third-Party Providers (CTPPs) and started direct examination of their risk and governance frameworks — with knock-on due-diligence obligations for every financial entity that relies on them.
- **Registers of Information are now a recurring obligation,** not a one-off project — financial entities must maintain and re-submit a full inventory of their ICT third-party arrangements to their regulator on an annual cycle.
- **Threat-Led Penetration Testing (TLPT) is live** for significant entities — live-environment, intelligence-led red-team testing on a roughly three-year cycle, run with accredited external testers, not a checkbox vulnerability scan.
- **Incident classification and reporting is being enforced on the clock** — major ICT incidents now require a phased notification to authorities (initial notification, intermediate update, final report), and late or inconsistent filings are increasingly treated as evidence of a weak underlying framework, not just a paperwork lapse.

The cost of getting this wrong

DORA gives national supervisors real enforcement teeth, and 2026 is the year they are being used. Beyond the headline fines, the operational cost of a gap — incident response that doesn't work under pressure, a critical vendor relationship with no exit plan, a board that can't answer basic questions about ICT risk — is usually far higher than the fine itself.

up to 2%	up to €5M	up to €1M
of total annual worldwide turnover — fines for financial entities	for designated Critical ICT Third-Party Providers	personal liability for individual managers, in certain member states

It shows up as business risk, not just fines
Regulatory: enforcement action, restricted activities, and mandatory remediation plans on a supervisor's timeline, not yours.

Commercial: enterprise and institutional clients increasingly require DORA evidence — a completed Register of Information, tested incident response, and audited third-party contracts — as a condition of doing business.

Operational: an ICT incident that isn't caught, classified, and reported correctly within the required windows compounds into a resilience failure, a reporting failure, and a governance failure at once.

Reputational: DORA findings are increasingly visible to supervisors across the EU through shared registers and cross-referenced reporting.

The five pillars of DORA

DORA is built on five interlocking requirements. Meeting one in isolation — a policy without testing, testing without a third-party register — does not satisfy the regulation, because supervisors now assess the framework as a whole.

Pillar	What it requires
1. ICT risk management	A governed framework to identify, protect against, detect, respond to, and recover from ICT risk — owned and approved at management-body level, not delegated to IT alone.
2. Incident management & reporting	Standardized classification of ICT-related incidents and a phased reporting process to regulators: initial notification, intermediate update, final report.
3. Digital operational resilience testing	Baseline testing (vulnerability scans, scenario-based testing) for all entities; live, intelligence-led Threat-Led Penetration Testing every ~3 years for significant entities.
4. ICT third-party risk management	A full Register of Information covering every ICT vendor relationship, contracts with mandatory exit and audit-rights clauses, and ongoing risk assessment of concentration risk.
5. Information sharing	Voluntary participation in cyber threat intelligence sharing arrangements across the financial sector to strengthen collective defense.

Compliance cannot be solved by lawyers alone

And operational resilience cannot be built through IT policies alone. That is the pattern we see across every organization preparing for DORA: the legal and compliance team can write the policy, and the technology team can hold the perimeter — but DORA asks for something neither can deliver on its own.

DORA sits exactly at the intersection of regulation, technology, cybersecurity, and business operations. A Register of Information is a legal obligation, but it can only be accurate if it is built from real, current infrastructure and vendor data.

Incident reporting deadlines are a regulatory requirement, but they can only be met if monitoring, detection, and escalation actually work end to end. Resilience testing is a compliance milestone, but it only means something if the systems being tested reflect how the business actually runs.

The goal: from “are we compliant?” to “are we actually ready?”

A completed policy binder answers the first question. It does not answer the second. Our approach is built to answer both — connecting the regulatory requirement to the technical and operational reality behind it, so that when a real incident, a real audit, or a real supervisory examination happens, the organization is not just documented — it is prepared.

The gaps we see most often

- **Incomplete or inaccurate Register of Information** — vendor and sub-contractor data scattered across procurement, IT, and legal, with no single owner and no process to keep it current year over year.

- **ICT risk frameworks** that exist on paper but were never tested against how systems are actually deployed and operated — especially in cloud and hybrid environments.

- **Third-party contracts missing DORA-mandated clauses** — exit strategies, audit rights, sub-outsourcing transparency — for vendors that were onboarded before the requirement existed.

- **Incident response plans** that have never been rehearsed under realistic conditions, so classification and the 24–72-hour reporting clock become a scramble instead of a process.

- **No clear line of sight from board-level governance down** to infrastructure-level controls — meaning the people accountable under Article 5 cannot actually evidence the oversight they are legally required to provide.

- **Resilience treated as a one-time certification project** rather than a continuously maintained state — leaving the organization compliant on the day of the audit and drifting out of compliance every day after.

DORA Operational Resilience & Compliance, by Gart Solutions

Gart Solutions is a cloud infrastructure, DevOps, and technical compliance consultancy. Our DORA Operational Resilience & Compliance service is built for one purpose: **to give EU financial organizations — and the technology vendors that serve them — an operational, evidence-backed path to DORA readiness, not just a policy document.**

We focus on the technical and operational backbone of DORA: ICT risk architecture, infrastructure and cloud resilience, third-party and vendor risk visibility, monitoring and incident response, and resilience testing support.

Who this is for

- **Banks, payment and e-money institutions,** and investment firms building or maturing their ICT risk framework ahead of supervisory review.
- **Insurers, fund managers, and trading venues** that need an accurate Register of Information and a tested incident response process.
- **FinTech, crypto-asset service provider**s, and platform operators that grew fast and now need to formalize resilience without slowing the business down.
- **ICT vendors and service providers** to the financial sector preparing for due-diligence questionnaires from clients now subject to DORA themselves.

Assess → Remediate → Sustain

We don't sell a one-time certification event, because DORA isn't one. Our engagement model mirrors how operational resilience actually has to be maintained: a fixed-scope diagnostic, a focused remediation phase, and an ongoing retainer that keeps the framework current as infrastructure, vendors, and threats change.

Phase	What happens	Outcome
1. Assess	Fixed-fee ICT risk, infrastructure, and third-party gap assessment mapped directly against DORA's five pillars — typically 2–6 weeks.	A prioritized, evidence-based gap report your board and regulator can both understand.
2. Remediate & Advise	Targeted project work to close the highest-risk gaps: risk framework build-out, infrastructure hardening, monitoring and incident-response design, Register of Information build.	Closed gaps, working controls, and audit-ready documentation.
3. Sustain	An ongoing retainer — continuous monitoring, annual Register of Information refresh, resilience-testing support, and governance reporting.	A framework that stays compliant as your organization and vendor landscape evolve.

Mapped to all five pillars

DORA pillar	How we help
ICT risk management	Risk framework design, governance mapping from board to infrastructure, cloud and infrastructure architecture review, Fractional CTO support for management-body oversight.
Incident management & reporting	Monitoring and detection design (SRE/IT Monitoring), incident classification workflows, response playbooks rehearsed against DORA's reporting timelines.
Resilience testing	Vulnerability assessments, scenario-based resilience testing, and coordination support for Threat-Led Penetration Testing with accredited providers.
ICT third-party risk	Register of Information build and maintenance, vendor risk assessment, concentration-risk analysis, and technical input into contract review alongside your legal team.
Information sharing	Guidance on participating in sector threat-intelligence sharing arrangements as part of a mature security operating model.

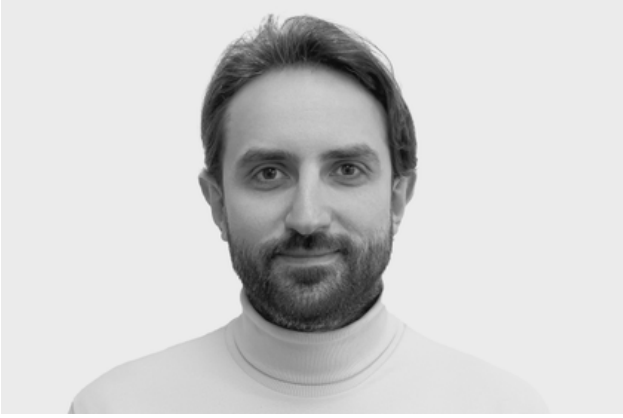
Why Gart?

Technical depth, honest scope

- **Cloud infrastructure and DevOps at our core** — resilience work grounded in how modern financial infrastructure is actually built and operated, not a generic policy template.
- **A track record in regulated environments** — technical compliance readiness work spanning ISO 27001, SOC 2, GDPR, NIS2, HIPAA/HITECH, and PCI-DSS, alongside infrastructure, security, and compliance audits.
- **A phased, fixed-scope entry point** — start with a fixed-fee assessment and a guaranteed, concrete gap report before committing to a larger remediation program.
- **Straight talk about scope** — we tell you clearly what's technical work we own and what needs your legal counsel, so nothing falls through the gap between the two.
- **A model built to last beyond the audit** — the Sustain retainer keeps your framework current as infrastructure, vendors, and the regulation itself continue to evolve.

gart.

Contributors



Fedir Kompaniiets

Co-Founder at Gart Solutions,
DevOps and Cloud Solutions Consultant

Roman Burdiuzha

Cloud Architect, Co-Founder and
CTO at Gart Solutions

gart.

Is DORA on your agenda?

Get in touch to discuss your current DORA readiness and next steps

gartsolutions.com

info@gartsolutions.com