

OPERATIONAL RESILIENCE

ACT (DORA).

DORA turns ICT risk into a board-owned, directly-regulated discipline across the EU financial sector — **and for the first time gives supervisors direct reach into the technology vendors, like cloud providers, that financial institutions depend on.**

- BOARD-LEVEL ICT ACCOUNTABILITY
- CRITICAL THIRD-PARTY OVERSIGHT
- THREAT-LED PENETRATION TESTING
- HARMONIZED INCIDENT REPORTING

01 THE MECHANISM



ICT Risk as Board-Level Accountability

DORA makes the management body directly and personally accountable for the ICT risk management framework — **a compliance program owned by IT alone doesn't satisfy the regulation**, since ultimate responsibility can't be delegated away from the board.



Direct Oversight of Critical Third Parties

For the first time, EU supervisors can directly designate and oversee “critical” ICT third-party providers, such as major cloud vendors. **A provider found non-compliant can trigger a forced exit** by every financial entity relying on it.



Threat-Led Penetration Testing

Significant entities must undergo live, red-team-style attacks on production systems under the TIBER-EU-based framework at least every three years — **testing a written plan is not the same as testing whether real systems survive an attack.**

02 THE FLOW

The DORA-Compliant Institution CONTAINED

1

The management body owns the ICT risk management framework directly, with board-level accountability that can't be delegated to IT alone.

2

Every ICT third-party contract is logged in a detailed register of information, with exit strategies defined before a critical vendor relationship, not after a failure.

3

Regular resilience testing, up to full threat-led penetration testing for significant entities, **validates the response plan against real attack behavior**, not just a document review.

The Fragmented, Untested Institution EXPOSED

1

ICT risk sits inside the IT department's own risk register, disconnected from board-level operational risk oversight, so systemic risk goes unseen at the top.

2

Third-party ICT relationships, including critical cloud dependencies, are tracked informally or not at all, so **a single vendor outage or breach becomes an unplanned crisis** instead of a modeled scenario.

3

Resilience is assumed rather than tested, so **the first real validation of the incident response plan happens during an actual incident**, not a controlled exercise.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
ICT Risk Management Framework	Requires a documented, board-owned framework covering ICT risk identification, protection, detection, response, and recovery, reviewed at least annually.
ICT-Related Incident Reporting	Classifies and reports major ICT-related incidents to competent authorities on a harmonized timeline, replacing a previously fragmented patchwork of sector-specific reporting rules.
Digital Operational Resilience Testing	Requires regular resilience testing for all entities, and threat-led penetration testing against live production systems for entities designated significant.
ICT Third-Party Risk Management	Governs contracts with ICT providers, including a mandatory register of information and defined exit strategies, with direct EU oversight of designated critical providers.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
IT Department Risk Ownership Alone	No	Without board-level accountability, ICT risk decisions compete for priority against the rest of the business instead of being treated as an enterprise risk.
Vendor Contracts Without a Central Register	No	Makes it impossible to assess concentration risk across critical ICT providers or respond quickly when one is compromised.
Tabletop Exercises Only, No Live Testing	No	Validates whether a team can talk through an incident, not whether the actual production environment withstands a real intrusion attempt.
Voluntary, Ad Hoc Incident Reporting	No	Leaves regulators and connected entities blind to the true scale and pattern of ICT incidents across the sector.
Board-Owned Framework + Central Third-Party Register + TLPT + Harmonized Reporting	Yes	Combines governance, vendor oversight, real-world testing, and regulatory visibility into a single enforceable structure.

OPERATIONAL RESILIENCE ACT (DORA). GOVERN · OVERSEE · TEST

05 PROGRAM OPERATIONS

DORA is a Regulation, not a Directive. It applies directly and identically across all EU member states with no national transposition, unlike earlier financial cybersecurity rules that varied by country.

DORA is lex specialis for the financial sector. Where it applies, it takes precedence over NIS2's general ICT risk rules for the same entity, rather than stacking as a second, overlapping obligation.

Critical ICT third-party oversight is a legal first. EU supervisors can now directly examine and sanction a technology vendor, such as a major cloud provider, that the vendor's own financial-entity customers depend on.

Proportionality doesn't mean exemption. Smaller and less complex entities get simplified requirements under DORA, not a waiver from the core risk management, reporting, testing, and third-party obligations.

06 CONTROL MAPPING

DORA (REGULATION (EU) 2022/2554)

The **core regulatory text**, directly applicable across the EU without national implementing legislation, in force since January 2025.

TIBER-EU FRAMEWORK

The **threat-led penetration testing methodology** DORA's advanced testing requirement is built on, using live red-team simulations.

JOINT ESA OVERSIGHT (EBA, ESMA, EIOPA)

The **three European Supervisory Authorities** that jointly develop DORA's technical standards and designate and oversee critical ICT third-party providers.

NIS2 DIRECTIVE

The **EU's general cybersecurity directive**, which DORA supersedes for financial entities under the lex specialis principle to avoid duplicate obligations.

07 WHAT THIS DOES NOT SOLVE

Non-ICT Operational Risk

DORA is scoped to **digital and ICT-related operational resilience**, not the full range of traditional operational, credit, or market risk a financial entity carries.

Data Protection Compliance

Managing ICT risk and reporting incidents under DORA doesn't itself satisfy **separate GDPR breach-notification and data-protection obligations**, which run on their own legal basis.

Non-Critical Vendor Risk

Direct EU oversight applies only to providers formally **designated critical** — the vast majority of ICT vendors remain the financial entity's own contractual responsibility to manage.

Global Reach Beyond the EU

DORA binds EU financial entities and their ICT providers, but doesn't extend supervisory authority over **ICT risk at entities operating entirely outside EU jurisdiction**.

08 MYTHS VS. REALITY

MYTH “DORA only applies to banks.”	REALITY DORA's scope spans banks, insurers, investment firms, payment institutions, and crypto-asset service providers — a far broader financial-sector reach than a banking-only rule.
MYTH “DORA is just another version of NIS2 for finance.”	REALITY DORA is more prescriptive and finance-specific, and explicitly overrides NIS2's general requirements for entities it covers rather than layering on top of them.
MYTH “Cloud providers are exempt because they aren't financial institutions.”	REALITY DORA specifically created a mechanism to directly designate and oversee critical ICT third-party providers, including cloud vendors, regardless of whether they're a financial entity themselves.
MYTH “A documented incident response plan satisfies the testing requirement.”	REALITY Significant entities must undergo live threat-led penetration testing against production systems — a plan on paper is not equivalent to a tested one.
MYTH “Smaller financial entities are exempt from DORA.”	REALITY Proportionality reduces the scope and intensity of some requirements for smaller entities, but the core obligations still apply — there's no small-entity exemption from DORA itself.

09 SPEAK THE PROGRAM — KEY TERMS

ICT RISK MANAGEMENT FRAMEWORK

The **board-owned governance structure** DORA requires for identifying, protecting against, detecting, responding to, and recovering from ICT risk.

CRITICAL ICT THIRD-PARTY PROVIDER (CTPP)

A vendor, such as a major cloud provider, formally designated by EU supervisors for **direct oversight due to its systemic importance** to the financial sector.

THREAT-LED PENETRATION TESTING (TLPT)

Live, **red-team-style attacks on production systems**, based on the TIBER-EU methodology, required for entities designated significant.

REGISTER OF INFORMATION

A detailed, regulator-facing inventory of **every ICT third-party contractual arrangement** a financial entity maintains.

LEX SPECIALIS

The legal principle under which **DORA's finance-specific rules take precedence** over the EU's general NIS2 cybersecurity directive for the same entity.

JOINT OVERSIGHT FORUM

The body through which the **three European Supervisory Authorities coordinate** direct oversight of designated critical ICT third-party providers.