CovertSwarm®

DORA: ARE YOU COMPLIANT, OR ARE YOU RESILIENT?

A guide for security and compliance leaders at UK and EU regulated financial institutions

THE QUESTION YOUR COMPLIANCE TEAM HASN'T ANSWERED

That question is the distance between compliance and resilience.

Your team has produced the documentation. The ICT risk framework exists. The Register of Information was submitted. The annual penetration test was signed off. The board approved a policy.

On paper, you are DORA compliant.

Here's the question nobody has asked out loud: has any of it been tested against real adversarial conditions?

Not scoped in advance. Not in a test environment. Not with the defenders briefed that something is coming.

Tested the way an attacker would test it.

Most firms in your position have closed the first gap and have not started on the second. That was an acceptable position in 2025. In June 2026, with formal supervisory assessments running across the EU and DORA findings feeding directly into capital requirement determinations, it isn't any more.

This guide names the specific places where DORA compliance commonly exists on paper and doesn't exist in practice. If any of them describe your current posture, you have a problem that more documentation will not solve.

WHAT DORA IS ACTUALLY MEASURING

DORA's five pillars (ICT risk management, incident reporting, resilience testing, third-party risk, and information sharing) are well-documented. What is less discussed is the operational standard they set.

The regulation is explicit about this in a way most compliance frameworks are not. It doesn't ask whether you have a testing programme. Article 24 asks whether your testing "assesses the preparedness for handling ICT-related incidents." Article 26 requires testing on "live production systems." The TLPT Regulatory Technical Standard (Delegated Regulation EU 2025/1190, in force July 2025) requires that the internal blue team is never aware the test is happening.

That last requirement is worth sitting with. The regulation doesn't just ask you to test. It asks you to test in conditions that reflect how attacks actually happen: without warning, against your real infrastructure, with defenders who have no advance knowledge.

That's not a compliance exercise. It's a test of whether your defences hold under those conditions, and whether the people responsible for your security would even know.

The distinction matters because most of what firms have built for DORA is compliance infrastructure. Documentation, registers, frameworks, board sign-offs. And regulators are now specifically looking for that gap.

01.
FIVE THINGS THAT LOOK LIKE DORA COMPLIANCE BUT ARE NOT.

THE ANNUAL PENETRATION TEST AS RESILIENCE TESTING COVERAGE

It is a point-in-time snapshot of a pre-agreed scope. That is not what Article 24 is asking for.

This is the most common mistake in the market right now.

A DORA-compliant testing programme under Article 24 requires independent testing of ICT systems supporting critical or important functions at least annually. Most firms read that and point to their existing annual penetration test. That test was scoped months before it ran. It covered what was agreed in a pre-engagement brief. It ran against a subset of your infrastructure under controlled conditions, with known parameters.

The EBA's published observations from the first Register of Information submissions (April 2025) flagged a directly connected pattern: firms were classifying core infrastructure as non-critical to shrink the scope of their regulatory obligations. An infrastructure that appears in your incident reports but isn't in your critical functions register is, in the EBA's own words, "not credible." That cross-referencing is now automated. If your testing scope and your criticality classification don't match your operational reality, the discrepancy gets escalated.

The annual pen test earns its keep as a baseline hygiene measure. It does not satisfy what DORA's testing pillar actually demands, and claiming it does is the kind of position that looks fine until a regulator asks to see the scope agreement.

A DOCUMENTED ICT RISK FRAMEWORK AS EVIDENCE OF BOARD GOVERNANCE

Article 5 is more specific than most firms have acknowledged.

It places direct accountability for ICT risk governance on the management body. Not the CISO. Not the security team. The board. Board members are expected to have demonstrable, current knowledge of ICT risk. And regulators are not taking policy sign-offs as evidence of this.

National competent authorities, including the Nordic NCAs who stated it explicitly, are reviewing board meeting minutes, approved ICT budgets, and evidence of board-level training to verify that governance is real and not ceremonial. A framework document approved at a board meeting and delegated entirely to the security function does not satisfy Article 5. It produces a paper trail that regulators are specifically trained to look through.

If your board cannot speak fluently to your ICT risk profile in a supervisory interview, that is not a presentation problem. Board members carry personal liability for governance failures under Article 5. The question regulators are asking isn't whether the policy exists. It's whether the people accountable for it can demonstrate they understand what it covers.

THE REGISTER OF INFORMATION AS A COMPLETED TASK

The RoI is not a task. It's a continuous obligation.

Forty-six percent of financial entities named the Register of Information as their single hardest DORA requirement in Deloitte's third compliance survey wave. The EBA's April 2025 observations documented the systemic problems with first-round submissions: invalid Legal Entity Identifiers, wrong file formats, blank sub-outsourcing templates for major cloud providers, and critical infrastructure classified as non-critical to narrow regulatory scope.

That last pattern is the one with the most direct enforcement consequence. The EBA introduced a Data Quality check layer in April 2026. NCAs are now automatically cross-referencing submitted RoI data against incident reporting histories. If your register categorises a service as non-critical and you have filed incident reports against it, the system flags the inconsistency and escalates it. There is no way to resolve that discrepancy with additional documentation. It requires either correcting the classification or explaining why the incidents were classified incorrectly.

The firms that treated the RoI as a submission to be completed and filed are now discovering that the regulator disagrees with their definitions of "critical."

INCIDENT REPORTING AS A DOCUMENTATION EXERCISE

DORA's incident reporting obligations under Articles 17 to 23 are procedural in a way that creates real operational risk.

Initial notification to your national competent authority is required within four hours of classifying a major ICT incident. Intermediate report within 72 hours. Final report within one month.

The classification criteria are specific and documented. The problem most firms have isn't that they don't know the rules. It's that their incident classification process hasn't been tested against the kind of event that would trigger the four-hour clock. When did you last run a live scenario against your major incident classification criteria? When did you last verify that the four-hour clock would actually start on time?

Regulators are already cross-referencing incident data against RoI submissions for consistency. The next level of scrutiny is whether firms' internal classification logs match what was reported, and whether reporting timelines were actually met. Late filing is an active enforcement priority. So is the pattern of under-reporting: classifying incidents below the major threshold to avoid the reporting obligation.

THIRD-PARTY CONTRACTS AS THIRD-PARTY RISK MANAGEMENT

You have mapped what was convenient to put in a spreadsheet.

Article 30 mandatory clauses (audit rights, regulatory access, exit strategies, sub-outsourcing notification), are not the same as managed third-party risk.

The 19 Critical ICT Third-Party Providers designated by the ESAs in November 2025, including AWS, Microsoft Azure, Google Cloud, IBM, Oracle, SAP, Salesforce, SWIFT, and FIS, are now subject to direct oversight. Their downstream financial institution clients are expected to have RoI entries that reflect the actual complexity of those relationships.

The Delegated Regulation on Subcontracting entered into force on 22 July 2025. Blank sub-outsourcing templates for AWS and Azure deployments were explicitly flagged in the EBA's observations as not credible. Every cloud deployment of material scale has downstream dependencies. If your register doesn't reflect them, you haven't mapped your actual risk.

Most firms have added the required clauses to new contracts and are working through their existing agreements. That's the contractual compliance position. The operational question is different: when did you last exercise an audit right? When did you last verify that a critical provider's sub-outsourcing arrangements match what they've told you? When did you last test an exit scenario?

02.
WHAT'S COMING, AND WHAT ENFORCEMENT LOOKS LIKE NOW.

THE TLPT OBLIGATION: WHAT'S COMING AND WHEN

For approximately 250 entities across the EU, the most operationally demanding DORA obligation is approaching.

TLPT notifications are expected to begin arriving in 2026. The first mandatory cycle deadline is 17 January 2028. Entities in scope are designated by their national TLPT Authority. You don't choose whether to participate. The designation criteria focus on globally and other systemically important institutions first.

When the notification arrives, the obligation is substantive: externally accredited testers (CREST satisfies Article 27), a Targeted Threat Intelligence report approved by your TLPT Authority, and a full red team exercise on live production systems with no advance warning to the blue team. The output is a formal regulatory attestation, not a penetration testing report.

There are two ways to be ready for a TLPT notification. The first: have a mature, continuously validated security posture, run regular adversarial exercises, and treat the TLPT as a formal attestation of resilience that already exists. The second: scramble to prepare a test programme you've never operated before, against live production systems, under regulatory oversight, with real consequences for what's found.

The notification gives you a window. It does not give you the foundation.

WHAT ENFORCEMENT ACTUALLY LOOKS LIKE NOW

The January 2026 shift in supervisory posture was real.

The ECB integrated DORA into its SREP methodology as of January 2026. ICT risk is now a dedicated supervisory module for approximately 113 directly supervised significant institutions. DORA findings feed directly into Pillar 2 capital requirement determinations. Non-compliance has a direct cost on your capital buffer. That is not a future scenario. It is the current supervisory framework.

National competent authorities including BaFin, DNB, CSSF, the Central Bank of Ireland, Finansinspektionen, the AMF, and others, are running formal evidence-based assessments with maturity scoring across four levels. Firms are receiving supervisory letters. Periodic penalty payments to compel compliance are being issued. The informal tolerance period that characterised 2025 is over.

A Veeam survey of European financial institutions published in August 2025 found 96% said they did not feel fully resilient under DORA's standards. Deloitte's third compliance survey wave found only 50% of regulated institutions expected to reach full compliance by the end of 2025. Those numbers don't describe laggards. They describe the industry average.

If your current position is that documentation exists and a review hasn't happened yet, you are in the majority. That majority is also the population currently receiving supervisory attention.

THE QUESTION TO ASK BEFORE THE REGULATOR DOES

The firms coming through DORA enforcement with their credibility intact are not the ones with the most comprehensive documentation. They are the ones that tested their posture before being asked to prove it.

The question worth asking now, while the answer is still yours to shape:

If an adversary with specific knowledge of your threat profile started probing your environment today, on live systems, without warning, would your controls hold? Would your third-party dependencies perform as documented?

If the honest answer is "we think so, but we haven't tested it that way," that's the gap DORA was written to close.

DORA findings now feed directly into Pillar 2 capital requirement determinations. The cost of the gap is no longer theoretical. It sits on your capital buffer, and it compounds if an incident closes it for you first.

THE CONVERSATION STARTS HERE.

If any of the five gaps in this guide describe your current posture, the useful next step is not more documentation.

CovertSwarm works with regulated financial institutions that have built their DORA compliance infrastructure and want to know whether the controls behind it would survive an adversary who hasn't read the scope agreement.

Our DORA Compliance Testing Assurance Review is a focused adversarial assessment: we test what you've built against the operational standard DORA actually enforces, identify where your tested resilience diverges from your documented resilience, and give you a clear picture of where you stand before a regulator or an incident does it for you.

CovertSwarm is a CREST-accredited offensive security firm. We hold CBEST and STAR-FS accreditation and are qualified to conduct DORA-aligned Threat-Led Penetration Testing under the Article 26 framework.

Learn more at covertswarm.com/contact-us

CovertSwarm Limited
International House
36-38 Cornhill
London
EC1A 2BN
United Kingdom

CovertSwarm Inc
1007 N Orange St,
4th Floor 333
Wilmington
Delaware, 19801
USA