REGULATORY INSIGHT

DORA at One Year: Reading the First Wave of Supervisory Findings

When the Digital Operational Resilience Act became applicable on 17 January 2025,[1] the prevailing question among financial entities was whether their frameworks would be ready in time. One year on, the question has changed. Supervisors have now completed their first full cycle of review, and the findings give firms something far more useful than a compliance deadline: a clear picture of what European regulators are actually looking at, where they are finding weaknesses, and how their expectations will sharpen in 2026.

This article reads that first wave of supervisory output — drawn from the European Central Bank's Supervisory Review and Evaluation Process, national competent authority stocktakes, the European Supervisory Authorities' reporting exercises, and direct supervisory guidance from BaFin and the Deutsche Bundesbank — and translates it into practical risk for in-house counsel and compliance teams.

From a Transition Year to a Supervisory Regime

It is worth being precise about what 2025 was. DORA applied in full from day one, with no formal transitional period. In practice, however, supervisors treated the year as a transition. National authorities and the ESAs adopted a risk-based, outcomes-focused posture: they reviewed frameworks, engaged directly with firms, identified gaps, and signalled expectations rather than moving immediately to enforcement. Two of the remaining Regulatory Technical Standards only entered into force in mid-2025, and the first list of designated critical ICT third-party providers was not published until 18 November 2025.[2] The architecture was still being completed even as firms were expected to operate within it.

That accommodation is now ending. Supervisors have described the next phase as a shift from “paperwork compliance” to “proof of operational resilience” — and, in BaFin's own framing, as a move toward genuinely interventionist supervision.[3] The first-year findings are best understood as the regulators showing their hand before that shift takes full effect.

The Register of Information Remains the Weak Link

If there is a single headline finding, it concerns the Register of Information. The Register — the structured inventory of every contractual arrangement for ICT services — is the dataset that feeds concentration analysis, CTPP designation, and the prioritisation of supervisory attention. It is, in effect, the map regulators use to decide where to look.

The data quality of that map has been poor. In the ESAs' 2024 dry-run exercise, just 6.5% of the roughly 1,000 participating firms passed all 116 of the data-quality validation checks.[4] The first official 2025 cycle

confirmed the underlying problem rather than resolving it: firms consistently underestimated the effort required to map third-party relationships accurately, capture subcontracting chains, and reconcile contractual detail across business lines. The 2026 cycle, with a reference date of 31 December 2025, was expected to demonstrate measurably more mature submissions.

The legal exposure here is easy to underrate. A Register that misstates dependencies is not merely an administrative defect — it can constitute a misrepresentation of the firm's risk profile to its supervisor, and it undermines every downstream obligation that relies on it.

Contractual Remediation Is Incomplete

Closely related is the state of the contract estate. Supervisors have observed that a substantial proportion of existing ICT contracts have not been updated to reflect DORA's minimum contractual requirements and the associated technical standards — including provisions on access and audit rights, subcontracting, service levels for critical or important functions, exit arrangements, and cooperation with authorities.[5]

This is a finding that lands squarely in the legal function. Repapering a vendor portfolio at scale is slow, depends on counterparty cooperation, and cannot be delegated wholly to procurement. Firms that have not completed contractual remediation, or that cannot evidence a credible, prioritised plan to do so, should expect this to feature in supervisory dialogue.

Incident Reporting: High Volume, Slow Detection

The major-incident reporting regime has generated significant traffic. National data points illustrate the scale — BaFin reported receiving more than 600 severe ICT incident notifications in the first year of DORA's application, equivalent to roughly twelve reports per week.[6]

The more pointed finding is qualitative. The BaFin and Deutsche Bundesbank IT-Aufsicht 2025 supervisory presentation reported that, in the slow-detection tail, the median time to detect an incident was fourteen days; operational disruptions were usually detected the same day, but cyber incidents were subject to a substantial detection gap.[7] Slow detection compresses the time available to classify an incident, meet DORA's strict notification deadlines, and mount an effective response. Authorities have also signalled that they expect firms to monitor their reporting *capability* on an ongoing basis, not simply to demonstrate it at the point of audit. Late or missing notifications sit at the top of every published list of likely early enforcement triggers.

ICT Risk Management and Governance Still Score Poorly

The ECB's 2025 SREP delivered an uncomfortable verdict: ICT risk received the worst average score across the assessed population, while operational risk scores remained largely stable.[8] After a year of intensive implementation activity, ICT risk management remained a persistent supervisory weak spot.

Supervisors have linked this to governance. The recurring criticism is that ICT risk frameworks exist on paper but are not yet embedded in the way the business is actually run — that boards are not consistently exercising the active ownership DORA requires, and that frameworks have not been translated into measurable, monitored controls. The emphasis on demonstrable board-level accountability is unlikely to soften.

Critical Third-Party Providers and Concentration Risk

On 18 November 2025 the ESAs published the first list of 19 designated critical ICT third-party providers, which now fall under direct oversight by Joint Examination Teams.[9] The list includes the major hyperscale cloud providers — AWS, Microsoft, Google Cloud, Oracle — alongside SAP, IBM, Bloomberg, LSEG Data & Risk, FIS, and a range of other financial-data and technology firms.

For financial entities, the designation reframes a familiar exposure. The BaFin and Deutsche Bundesbank IT-Aufsicht 2025 supervisory presentation drew explicit attention to market concentration around a small number of providers and to the frequent absence of credible, tested exit strategies.[10] A dependency on a designated CTPP is not in itself a deficiency, but a dependency that is undocumented, unquantified, or unaccompanied by a realistic substitutability plan is precisely the kind of finding the oversight regime is built to surface.

Testing Moves from Policy to Proof

Resilience testing is the area where the change in supervisory posture is clearest. Threat-led penetration testing for entities identified as significant operates on a multi-year cycle, and the Register data submitted in 2026 will help determine which firms are selected. Supervisory guidance has also begun to set concrete expectations around the operational disciplines that underpin resilience — binding remediation deadlines for patch and vulnerability management, centrally monitored compliance, and demonstrable plans to meet defined recovery time and recovery point objectives.[11] The direction of travel is from testing as a documented programme toward testing as evidenced effectiveness.

What the Findings Tell Us About 2026

Read together, the first-year findings point to a consistent supervisory thesis: many firms have the documentation but not yet the demonstrable operational reality. Deloitte's 2025 European DORA Survey reported that only around half of regulated entities expected to reach full compliance by year-end 2025, with a further substantial share targeting 2026 — meaning a meaningful portion of the sector entered the enforcement phase with known, unremediated gaps.[12]

The consequences of remaining in that group are no longer theoretical. DORA's sanctioning framework (Articles 50–52, Chapter VII) allows for significant administrative penalties, alongside supervisory powers to require remedial measures, conduct on-site inspections, and publicise breaches — implemented

divergently across Member States.[13] The early enforcement focus has been clearly telegraphed: incident reporting failures, inadequate ICT risk frameworks, contracts missing required clauses, testing deficiencies, and governance gaps.

Practical Priorities for Financial Entities

For firms reassessing their position against the first wave of findings, several priorities stand out:

- **Treat Register of Information accuracy as a legal risk, not a reporting task.** Reconcile the Register against actual contracts and dependency maps, capture subcontracting chains, and ensure the picture it presents to your supervisor is one you can defend.
- **Complete and evidence contractual remediation.** Where repapering is incomplete, maintain a documented, risk-prioritised plan with timelines — the plan itself is part of your supervisory story.
- **Audit detection and notification capability, not just policy.** Test how quickly incidents are identified, classified, and escalated against DORA's deadlines, and monitor that capability on a continuing basis.
- **Make board ownership demonstrable.** Ensure ICT risk reaches the board with substance, and that decisions, challenge, and oversight are recorded.
- **Quantify and plan for third-party concentration.** For dependencies on designated CTPPs, document the exposure and develop realistic, tested substitutability and exit arrangements.
- **Shift testing from documentation to evidence.** Align vulnerability management, recovery objectives, and resilience testing so that effectiveness — not merely the existence of a programme — can be shown.

Conclusion

DORA's first year was a stocktake. The second will be a test. The supervisory findings published so far are unusually candid about where the sector falls short, and that candour is an opportunity: firms now have a detailed, regulator-validated checklist of the issues most likely to attract scrutiny. The entities that fare best in 2026 will be those that read these findings not as criticism of the past year, but as a precise specification of what supervisors expect to see next.

References

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), OJ L 333, 27 December 2022, p. 1.
2. EBA, EIOPA and ESMA, joint press release, *"European Supervisory Authorities designate the first critical ICT third-party service providers under the Digital Operational Resilience Act"* (18 November 2025).
3. Speech by R. Speer (BaFin), *"Das erste Jahr DORA"* (4 December 2025), bafin.de.

4. ESAs, *Summary Report — DORA Dry Run exercise on Registers of Information* (ESA 2024 35, December 2024), reporting that 6.5% of the ~1,000 participating firms passed all 116 data-quality validation checks.
5. BaFin (n 3); BaFin/Deutsche Bundesbank, *IT-Aufsicht im Finanzsektor 2025 — Vortrag 1* (December 2025), on the remediation of ICT contracts to DORA's minimum contractual requirements.
6. BaFin (n 3), reporting more than 600 severe ICT incident notifications in the first year of DORA's application.
7. BaFin/Deutsche Bundesbank (n 5), on detection times for ICT incidents.
8. European Central Bank, Banking Supervision, *Aggregated results of the 2025 Supervisory Review and Evaluation Process (SREP)* (18 November 2025); see also ECB, *Supervisory priorities for 2026–2028* (18 November 2025).
9. EBA, EIOPA and ESMA (n 2); Commission Delegated Regulation (EU) 2025/420 on Joint Examination Teams.
10. BaFin/Deutsche Bundesbank (n 5), on concentration around a small number of providers and the absence of tested exit strategies.
11. BaFin/Deutsche Bundesbank (n 5), on supervisory expectations for vulnerability management deadlines and recovery objectives.
12. Deloitte Luxembourg, *DORA European Survey — 2025 edition*, reporting that 50% of the 36 surveyed financial entities (across 28 countries) expected full DORA compliance by end-2025, with 38% targeting 2026.
13. DORA (n 1), Articles 50–52 (Chapter VII — administrative penalties, remedial measures, and the reservation of Member State criminal penalties); DLA Piper, *"Divergence in administrative penalties under DORA"* (October 2025), on cross-jurisdictional implementation.
