InfoSecAI

A BRIEF FOR FCA / CBI-REGULATED FIRMS

REALITY CHECK · 2026

DORA — The 12-Month Reality Check.

What FCA and Central Bank of Ireland regulated firms have learned in the first year of DORA enforcement. A pillar-by-pillar self-check for boards, CISOs and risk leads in financial services.

AUTHORED BY

Paul Jolliffe

Founder & Director, InfoSecAI · Senior CISO / vCISO · FCA-aligned environments · CISSP · ISO 27001 Lead Auditor · MBA

01 · 12 MONTHS IN

The audit phase has begun.

DORA — Regulation (EU) 2022/2554 — has been in force since 17 January 2025. The transitional honeymoon is over. Competent authorities across the EU are now examining: incident reports submitted, third-party registers maintained, threat-led penetration testing scoped, board minutes evidencing governance. **Firms that staged an implementation programme but did not maintain it are starting to fail those examinations.**

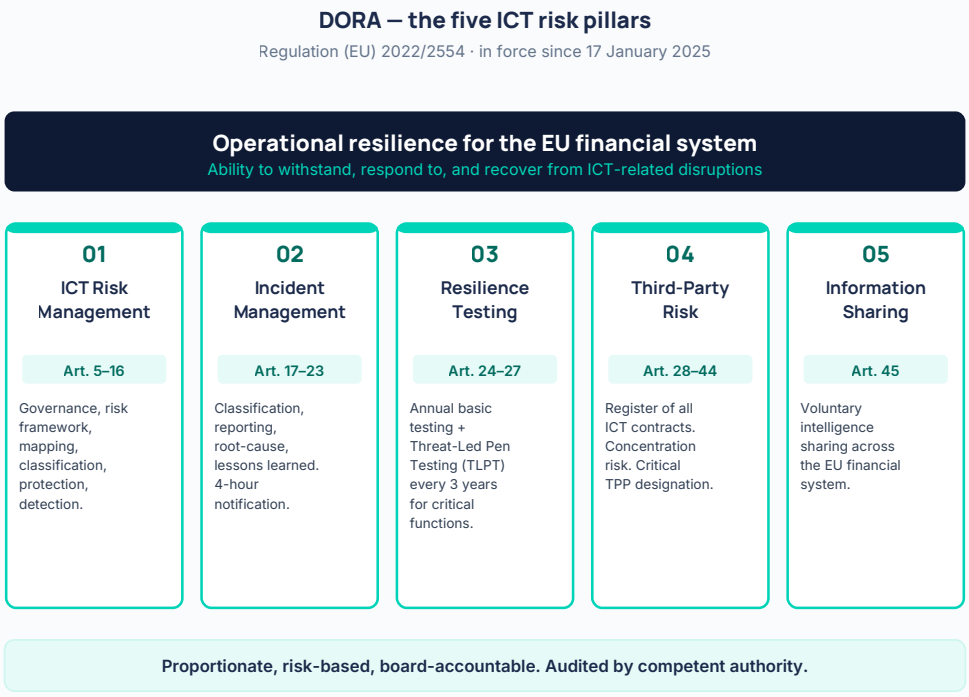
This brief sets out what I am seeing on the ground in regulated firms across the UK and EU — the gaps that consistently appear, the areas regulators are now drilling into, and the artefacts that need to be in place if you are examined this year. Where applicable, I have pulled across the equivalent UK FCA Operational Resilience expectations, since the two regimes increasingly mirror each other for cross-border firms.

> **Reading note.** If you are a board member or audit committee chair, the five-pillar overview, the third-party matrix and the incident timeline are the priority pages. If you are a CISO, risk lead or DORA programme owner, the gap analysis and self-check questions will save the most time.

02 · THE FIVE PILLARS AT A GLANCE

Five pillars. One operational resilience objective.

DORA is structurally simple even though its detail is dense. Five pillars carry the substantive obligations, supported by Regulatory Technical Standards and Implementing Technical Standards across each.



The five pillars of DORA. Boards should be able to articulate where the firm sits against each.

Pillars 1 & 2 — ICT risk management and incidents.

Pillar 01 · ICT Risk Management (Articles 5–16)

QUESTION	STATUS (RAG)	EVIDENCE ARTEFACT
Has the management body approved the ICT risk management framework, and does it review it at least annually?	—	Board minutes; framework v-controlled.
Is there a documented ICT business continuity policy and a tested disaster recovery plan covering all critical or important functions?	—	BCP / DRP, last test report.
Have all critical or important functions been identified, classified and mapped against supporting ICT systems?	—	Function register with ICT linkage.
Is there an information / cyber threat intelligence function feeding the risk framework?	—	Intel briefs, CTI procedure.
Are vulnerability management, patching, hardening and capacity planning operating with documented SLAs?	—	SLA dashboards, exception register.
Is there an annual ICT-risk audit programme covering critical functions?	—	Internal audit plan, sample reports.

Pillar 02 · ICT-related Incident Management (Articles 17–23)

QUESTION	STATUS (RAG)	EVIDENCE ARTEFACT
Is there a documented incident classification process aligned to the seven RTS criteria (clients, reputation, duration, geography, data, services, economic)?	—	Classification SOP, training record.
Can the firm demonstrate a 4-hour initial notification capability to the competent authority?	—	Tabletop record, on-call rota.
Are post-incident reports filed within the 1-month deadline with full root-cause analysis?	—	Final reports filed.
Are major incident lessons fed back into ICT risk and supplier review?	—	Steering minutes, action register.
Is there a defined customer / counterparty notification protocol for material incidents?	—	Comms plan, sign-off matrix.

Pillars 3, 4 & 5 — Testing, third-party, info-sharing.

Pillar 03 · Digital Operational Resilience Testing (Articles 24–27)

QUESTION	STATUS	EVIDENCE ARTEFACT
Is there an annual ICT-resilience testing programme covering all critical functions?	—	Test plan, results.
If in scope for TLPT (Threat-Led Pen Testing), has the 3-yearly cycle been planned with the competent authority?	—	TLPT cycle plan, regulator engagement.
Are findings from testing tracked, remediated and re-tested with traceability?	—	Findings register, retest evidence.

Pillar 04 · ICT Third-Party Risk Management (Articles 28–44)

QUESTION	STATUS	EVIDENCE ARTEFACT
Is the Register of Information of all ICT third-party arrangements maintained and submitted to the regulator on schedule?	—	Register submission, version control.
Is contractual content for all ICT services compliant with Article 30 minimum requirements?	—	Contract review log, exception register.
Is supplier concentration risk assessed and reported, especially for critical or important functions?	—	Concentration analysis, board paper.
Is there an exit strategy for each critical or important supplier, including alternative providers?	—	Exit plans on file.
Are critical TPP arrangements subject to enhanced due diligence and ongoing monitoring?	—	Annual review records.

Pillar 05 · Information Sharing (Article 45)

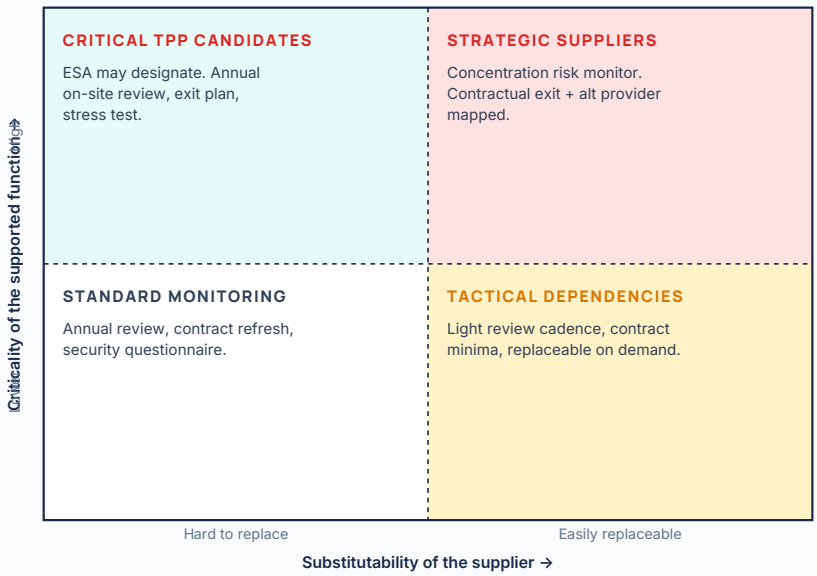
QUESTION	STATUS	EVIDENCE ARTEFACT
Has the firm joined or considered joining a sector intelligence-sharing arrangement?	—	Membership documentation.
Are there documented data-protection safeguards covering shared intelligence?	—	Sharing protocol, GDPR review.

Concentration is what the regulator is examining.

Article 28 requires every ICT third-party arrangement to be registered. The competent authority then expects you to identify which are **critical or important**, and to manage concentration on the supplier side. This is where I see the most consistent gap: registers exist but the criticality assessment is light, exit plans are aspirational, and concentration is not articulated to the board.

Third-party ICT criticality matrix

DORA Art. 28: every ICT third-party contract registered. The matrix tells you which need deep oversight.



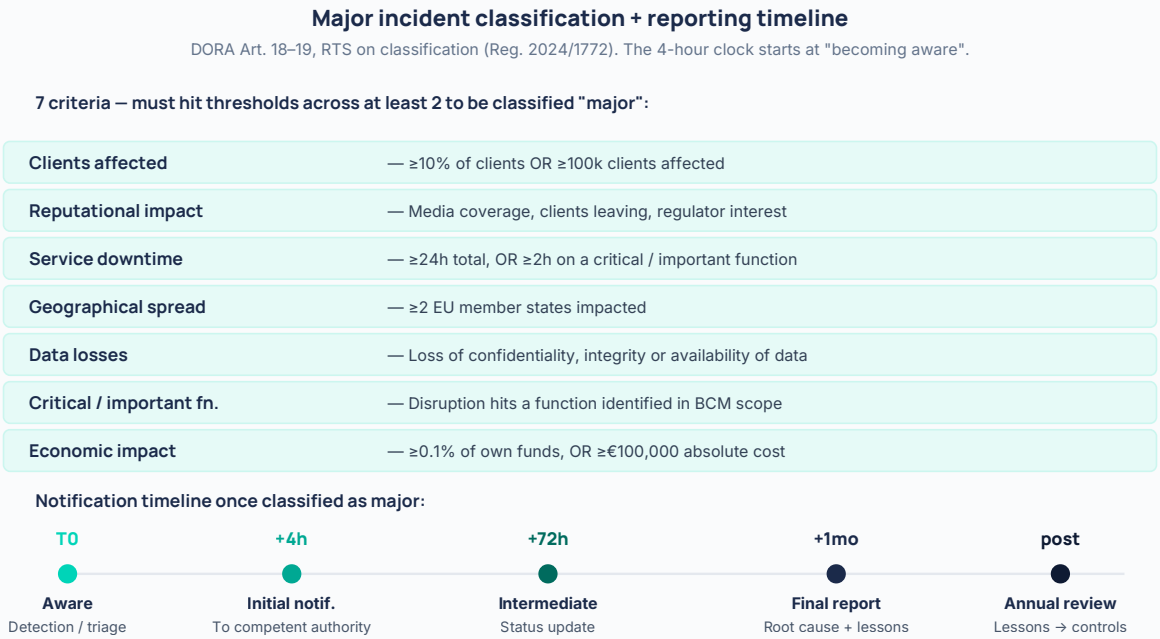
The criticality matrix that should sit alongside every third-party register. The top-right is where regulators concentrate their examination.

> **Practitioner observation.** If your firm runs core or critical services on a single hyperscaler with no realistic alternative provider, the regulator will expect to see this acknowledged in the board pack and an exit plan that is operationally credible — not a paragraph in a contract.

05 · MAJOR INCIDENT CLOCK

The 4-hour clock starts at "becoming aware".

Incident classification and reporting is the single most operationally tested area of DORA in 2026. Firms that went through a major incident in 2025 found the 4-hour notification clock unforgiving — and the seven RTS criteria less intuitive in the heat of the moment than they look on paper.



The seven classification criteria and the four-stage notification timeline. Build this into your incident playbook, not your DORA programme document.

06 · THE SEVEN GAPS I KEEP SEEING

Common implementation gaps observed in 2026.

From advisory engagements across UK and Irish FCA / CBI-regulated firms in early 2026, these are the gaps that come up most often. None are esoteric. All are correctable.

THE GAP	WHAT IT LOOKS LIKE	HOW TO CLOSE IT
Register of Information is incomplete	Top-tier suppliers captured; SaaS sub-suppliers and group services missing.	One canonical register sourced from procurement, finance and IT; reconciled quarterly.
Critical / important function map is aspirational	Functions identified at a high level; mapping to ICT systems and to suppliers is partial.	End-to-end function-to-system-to-supplier traceability; refreshed at least annually.
Incident classification has not been rehearsed	Policy exists; on-call team would struggle to apply the seven criteria within four hours under pressure.	Two tabletops a year using the seven criteria; a one-page cheat sheet on the IR runbook.
TLPT readiness is unclear	Firm is not sure if it is in TLPT scope; if it is, the 3-yearly cycle has not been planned with the regulator.	Confirm scope with competent authority; set the cycle and get budget approved.
Exit plans are paragraphs, not playbooks	Contracts have exit clauses; operational exit playbooks for critical hyperscaler services do not exist.	Draft a credible operational exit for each critical TPP; rehearse desktop annually.
Board reporting is policy, not posture	Audit Committee receives quarterly DORA "status updates"; it cannot articulate residual risk.	Board pack moves from green/amber/red status to residual-risk and decision-driven format.
Lessons are not being fed back	Incidents happen, post-mortems happen, but the improvements do not always appear in the next risk review.	Post-mortem actions tracked alongside the risk register; quarterly closeout review.

07 · ABOUT INFOSECAI

If your DORA position needs a senior lift.

InfoSecAI provides fractional CISO, vCISO and senior security advisory services to UK and EU organisations, including FCA-regulated and dual-regulated firms. We help boards, executives and security leaders deliver practical operational resilience and DORA conformance.

FCA
regulated experience

DORA
programme advisory

£12m
largest cyber programme delivered

Run the full self-check in the InfoSecAI DORA Copilot — launching Q3 2026.

Pillar-by-pillar self-check, Register of Information builder, function-to-supplier traceability, board posture pack — all in one guided web workspace.

- **~50 questions** across the five pillars, RAG-rated, with implementation guidance.
- **Register of Information builder** aligned to Article 28 and related ITS.
- **Critical function mapper** — function → system → supplier traceability.
- **Board posture pack** — auto-drafted, residual-risk and decision-driven format.

Email **paul.jolliffe@infosecai.net** to join the early-access list.

To talk about your DORA position

A 30-minute conversation about where your firm sits against each pillar, the one or two gaps that would cause the most regulator concern in an examination, and whether a fractional or programme advisory model is the right shape. No charge, no obligation.

Email paul.jolliffe@infosecai.net or book directly: infosecai.net.

Founder credentials: MBA (Henley Business School) · CISSP · ISO 27001:2022 LA / LI / IA · PRINCE2 Practitioner. Past engagements include IBM, KPMG, PwC, T-Systems (Deutsche Telekom), Philip Morris International, Britannia Financial Group (FCA-aligned), MTN, Phoenix Software, Lloyds Banking Group.