

From Self-Assessment to Supervisory Scrutiny

What UK operational resilience now requires, and where DORA genuinely applies



What one year of supervisory review found

The transition period under the FCA's operational resilience rules, PS21/3, and the PRA's SSI/21 ended on 31 March 2025. Many institutions treated that date as a finish line: identify important business services, set impact tolerances, complete mapping and scenario testing, submit the self-assessment, move on to the next priority.

In March 2026, the FCA published its findings after a year of reviewing firms' annual self-assessments, and the results argue against that reading. The regulator found self-assessments that had not been updated since March 2025, even where a firm had migrated a core platform or changed a material outsourcing arrangement in the meantime. It found testing evidence that amounted to a summary report rather than the scenario design, participant lists and timing data the FCA now expects to see. It found remediation plans recorded but not funded, governed, or retested to confirm the vulnerability was actually closed.

The message from the regulator is explicit: this is an ongoing discipline, not a project with a delivery date. Boards are expected to show genuine engagement with the self-assessment, not simply approve it.



Where DORA fits, and where it doesn't

It is worth being precise here, because the two regimes get conflated often enough that the confusion is itself a source of risk. DORA is EU law. It binds UK institutions only where they operate an EU-regulated entity, run an EU branch, or provide ICT services into EU-regulated financial entities. A UK-only bank or building society with no EU footprint is not a DORA entity, and treating it as one diverts effort from the regime that actually applies: PS21/3 and SSI/21, alongside new incident reporting rules from the Bank of England, PRA and FCA that take effect in March 2027.

For institutions with genuine EU exposure, DORA's Register of Information and third-party risk management requirements do apply, and are under active supervision in 2026, with national competent authorities cross-checking submissions and beginning enforcement action. That subset of the estate needs its own workstream. It should not set the framing for the rest of the institution's resilience programme.



Why the architecture is the actual constraint

Ask a Head of Operational Resilience where the evidence gaps sit, and the honest answer is rarely that the requirement is misunderstood. It is that the evidence can't be produced at the granularity the requirement now asks for. Impact tolerances are set per important business service, but a monolithic core rarely maps cleanly onto individual business services. Dependency mapping needs to trace a specific service through specific infrastructure and specific third parties, and a tightly coupled architecture turns that tracing into a manual, point-in-time exercise rather than something the system can report on continuously.

This is an architecture problem wearing a compliance costume. An API-led, service-oriented core makes it possible to instrument evidence generation at the level the regulator is now asking for: continuous, tied to a specific service, and generated as a by-product of how the system runs rather than assembled retrospectively before an exam.



What automated compliance evidence looks like in practice

A DevSecOps pipeline built for a regulated environment runs static and dynamic application security testing, secrets management, mutual TLS and role-based access control at every stage of CI/CD, and generates PCI-DSS, GDPR and operational resilience evidence on every build and deployment rather than once a year ahead of a self-assessment deadline. Testing records, scenario participant data and remediation closure evidence accumulate as the system runs, through a dedicated observability layer, rather than as a separate exercise someone has to remember to do each February.



What this looks like under a real outage

One live engagement shows what continuous resilience evidence actually produces. Maveric built a graceful-degradation layer for a bank's API platform that keeps login, account summary, account details and transaction history available to customers even when a backend or host system is down for maintenance, rather than returning an error. The same programme brought API certification down to seven days per API and caught 70 percent of defects through automation before they reached production, and the client has since onboarded more than 20 fintech partners across 14 markets on top of that resilient layer.

That is the kind of evidence a self-assessment can point to directly: a specific mechanism, tested, with a measured outcome, rather than a policy document asserting the capability exists.

Sources: FCA, "Operational resilience: insights and observations one year on" (March 2026); FCA/PRA/Bank of England incident reporting rules, PS26/2 (in force March 2027); DORA scope analysis for UK firms, Mitratech and FluxForce (2026).



If this raises questions about your own posture

We're glad to talk through where DORA does and doesn't apply to your institution specifically. No pitch attached, just the read on where you stand.

The Maveric Edge

Maveric Systems is a banking-exclusive technology specialist with 25+ years of domain expertise, engineering trust in AI-first banking. We deploy AI at the core through our proprietary AI@Scale framework and AI-powered platforms, guided by principles that engineer trust by design. Our pragmatic, outcome-driven approach, and AI services spanning advisory, CoE establishment and specialist competencies led engagements make us the trusted engineering partner for the AI era.