803 HOURS DOWN: UK BANKING'S OPERATING MODEL FAILURE

803 hours of unplanned downtime. 158 IT failure incidents. 9 major banks and building societies

FOREWORD

Between January 2023 and February 2025, the Treasury Select Committee compelled nine of the UK's largest banks and building societies to disclose their IT failure records.

The data published in March 2025 was extraordinary, not because the numbers were surprising, but because of what those numbers reveal when viewed through an operating model lens.

These were not isolated incidents. They were not bad luck. They were the predictable output of an operating model designed for compliance, not for resilience.

The most common causes cited by the banks themselves: problems with third-party suppliers, disruption caused by changes in systems, and internal software malfunctions.

This is not a technology problem. It is the supplier model and transition management failures that OMDDMS® has catalogued as structural failure modes, expressed in nine banks, across two years, as 803 hours of downtime.

> ***"For families and individuals living paycheck to paycheck, losing access o banking services on payday can be a terrifying experience." – Dame Meg Hillier MP, Chair. Treasury Select Committee. March 2025***

THE EVIDENCE

The nine institutions named in the Treasury Committee's correspondence were Barclays, HSBC, Lloyds Banking Group, Nationwide Building Society, Santander UK, NatWest Group, Danske Bank, Bank of Ireland UK, and Allied Irish Banks.[1]

Each was required to disclose, in writing to the Committee, the number of incidents and total hours of unavailability their customers experienced over the two-year period.

803
HOURS OF UNPLANNED DDOWNTIME

158
IT FAILURE INCIDENTS

9
BANKS & BUILDING SOCIETIES

£12.5m
BARCLAYS POTENTIAL COMPENSATION

Where banks provided a clear aggregate figure, the disclosures were stark. NatWest reported 194 hours of customer impact across 13 incidents - the majority of that figure, some 142 hours, attributable to a single event.[4]

Danske Bank reported a cumulative duration of 113 hours and 56 minutes across five incidents, although the bank noted that around 60 of those hours fell within a weekend period when its CHAPS payment scheme was not operating.[5]

Barclays disclosed 93 hours of channel-impacting downtime across 15 incidents, separate from the high-profile three-day outage at the end of January 2025, which was reported individually and is not included in that total.6 Nationwide reported 70 hours and 26 minutes across 18 incidents.[7]

Bank of Ireland UK disclosed roughly 22 hours of quantified downtime across three incidents, plus two further incidents involving payment-processing delays for which no duration was stated.[8]

THE EVIDENCE (contd.)

Not every institution disclosed its figures in a directly comparable way.

Santander UK reported impact by channel rather than by incident, with cumulative per-channel outage time totalling in the region of 116 hours across 24 incidents[9] - a methodology that makes like-for-like comparison with the other banks difficult.

HSBC and Lloyds Banking Group's letters to the Committee did not yield a single, clearly stated aggregate downtime figure in the material reviewed for this article.

This inconsistency is itself part of the story.

Nine regulated institutions, asked the same questions by the same Parliamentary committee, used at least three different methodologies to measure and report something as fundamental as "how long were our customers unable to bank with us."

That is not a reporting failure at the margins.

It is what happens when operational resilience has never been designed as a single, comparable, governed capability - which is exactly the gap PS26/2 is intended to close from March 2027.

THE REGULATOR'S VERDICT

The FCA reviewed what firms actually did. What it found was an operating model problem.

In March 2026, exactly one year after the compliance deadline, the FCA published its review of firms' annual self-assessments (*Operational Resilience: Insights and Observations One Year On*, 27 March 2026).[2] The regulator did not use the phrase 'operating model failure' but that is precisely what it described.

The FCA's findings are structured around six components. Read without regulatory language, they map onto the same structural failure modes that appear in every sector, every time.

1

IMPORTANT BUSINESS SERVICES AND IMPACT TOLERANCES

Firms set impact tolerances but could not demonstrate they would remain within them under real stress. The FCA found that tolerances were often set equal to current recovery times rather than grounded in genuine harm analysis, measuring what the firm does, not what its customers can bear.

2

MAPPING

Firms mapped technology. They did not map people, process, facilities, or third-party dependencies, the operating model beneath the systems. Where third parties were included, mapping stopped at the contractual boundary. The chain of fourth- and fifth-party dependencies remained invisible.

3

SCENARIO TESTING

Scenario testing lacked depth and severity. Some firms' self-assessments stated there was no scenario they could not recover from without evidence of having tested scenarios severe enough to challenge that claim. The FCA expects testing to identify scenarios that would breach impact tolerances, not merely confirm existing assumptions.

THE REGULATOR’S VERDICT

4

VULNERABILITY MANAGEMENT

Some less mature firms reported no vulnerabilities at all, a finding the FCA treated not as evidence of strength but as evidence of insufficient testing. Where vulnerabilities were identified, remediation tracking was weak: actions were logged but not owned, not sequenced, and not closed.

5

COMMUNICATIONS

Communications plans existed on paper but had not been tested against conditions where normal channels fail, precisely the conditions that occur during a live incident. Firms asserted resilience in their communications approach without evidence of having stress-tested it.

6

SELF-ASSESSMENT

Where self-assessments were overly high-level or lacked supporting evidence, boards were less well-placed to exercise effective oversight or form a clear view of residual risks. The FCA expects self-assessments to be sufficiently detailed for the board to understand the firm’s resilience position, challenge assumptions, and prioritise investment not to provide a narrative of confidence without the evidence to support it.

The regulator can mandate what resilience requires. It cannot mandate how to design the operating model that delivers it.

THE FIVE FAILURE MODES

1 Resilience treated as an output, not a design constraint

WHAT THE FCA FOUND	OMDDMS® DIAGNOSIS
Firms completed resilience mapping as a compliance deliverable after systems, products, and processes were already built. The operating model was the output of the programme, not the framework within which it was designed.	Resilience is not a control that sits alongside your operating model. It is a property of your operating model. Firms that treat it as a post-build exercise will always be documenting fragility rather than designing out of it.

2 Governance designed for accountability, not decisions

WHAT THE FCA FOUND	OMDDMS® DIAGNOSIS
Boards could not demonstrate clear understanding of their operational resilience responsibilities. Governance structures specified who attended; they did not specify who decided, on what basis, or with what authority to act.	Good governance is not about who is in the room. It is about what they are empowered to decide. When governance is built around reporting rather than decision rights, the board receives information without the authority to act on it. Issues surface, are discussed, and surface again.

THE FIVE FAILURE MODES

3 Capability treated as a training problem

WHAT THE FCA FOUND	OMDDMS® DIAGNOSIS
Mapping focused almost entirely on technology. People, process, facilities, and third-party dependencies were insufficiently documented. Firms could not demonstrate the structural capability to remain within impact tolerances only the procedural intention.	Capability is a design question before it is a development question. Knowing what your technology stack does is not the same as knowing whether your people, processes, and supplier relationships can sustain your critical services when that stack fails. The FCA found firms mapping the former and assuming the latter.

4 Transition managed as a communications exercise

WHAT THE FCA FOUND	OMDDMS® DIAGNOSIS
Communications plans existed but were not tested as part of scenario exercises. Firms had not designed what happens when their usual communication channels fail during a live incident, the moment when communications matter most.	A communications plan is not a resilience plan. Resilience requires designing what the organisation does, not just what it says. The transition from normal operations to disrupted operations and back is a design problem, not a messaging challenge. Firms that treat it as the latter will discover that distinction during a live outage.

THE FIVE FAILURE MODES

5	The operating model declared complete at go=live
WHAT THE FCA FOUND	**OMDDMS® DIAGNOSIS**
The March 2025 deadline was treated as the endpoint. The FCA's review found firms carrying 'compliance debt': static self-assessments, point-in-time mapping, and scenario tests that did not update as the business changed. The regulator's own conclusion: 'Operational resilience is not static.'	An operating model is a living system. The moment a programme closes and the budget disperses; the operating model begins encountering the reality it was never designed against. In banking, that reality is 803 hours of downtime and a regulator that is now watching. The cost of this failure mode is not the outages. It is the March 2027 reporting deadline that nobody designed an operating model to meet

THE 2027 DEADLINE

On 18 March 2026, the FCA and PRA published new mandatory incident reporting requirements (FCA PS26/2 and PRA PS7/26), with the Bank of England publishing parallel requirements for financial market infrastructures. All come into force on 18 March 2027.[3] Firms had 12 months to prepare.

WHAT THE RULES REQUIRE

- Report all operational incidents within 24 hours of determining a threshold has been met (4 hours for payment services)
- Maintain a register of all material third-party arrangements and submit the register annually via a standardised format through a single portal — Chief Operations function (SMF24) holds personal accountability

WHAT THIS DEMANDS OPERATIONALLY

- A defined process for identifying when a reporting threshold has been breached — before an incident, not during one
- Clear decision authority for who triggers a report. Real-time visibility of third-party dependencies across the supply chain
- An operating model that treats reporting as a live function, not a retrospective exercise

THE 2027 DEADLINE

WHAT MOST FIRMS ARE BUILDING

A reporting template. A notification workflow . A new compliance workstream . The same operating model, with a new form on top of it

The operating model gap that caused 803 hours of downtime will not be closed by a reporting portal. It requires operating model design.

OMDDMS® provides the only globally accredited standard for designing, delivering, and managing operating models.

Oliver Swift is one of two organisations accredited to train it. If your firm is preparing for March 2027, this is where capability begins.

> ***“That twelve-month window was sufficient for firms that started immediately. It is almost certainly insufficient for firms that treat March 2027 as the point at which preparation begins, which is precisely the pattern the FCA documented in the March 2025 deadline.” - Austin Merrett, Founder and Director, June 2026***

QUESTIONS FOR PROGRAMME AND PROJECT LEADERSHIP

If your team can answer these confidently, the operating model is being managed. Most cannot.

1	Is operational resilience built into the design of this programme, or is it a workstream we will add before go-live?
2	Does our governance structure specify who has authority to make decisions under disruption — or does it specify who attends the meeting?
3	Have we mapped the people, processes, and third-party relationships our critical services depend on, or have we mapped the technology and assumed the rest will follow?
4	Have we designed and tested what happens when our usual communication channels fail during a live incident or have we written a communications plan?
5	Who is accountable for maintaining the operating model after go-live, and is that person funded, empowered, and named in the project plan?

THE REGULATOR IDENTIFIED THE GAPS

Most operational resilience programmes fail at the same point: the operating model is treated as something that emerges from the project, rather than something the project is designed to produce. OMDDMS® reverses that. It is the only globally accredited standard built specifically for operating model design, delivery, and management and the structured approach it provides maps directly onto every failure mode the FCA identified.

Without it, firms are designing resilience by instinct. With it, they are applying a proven methodology with defined components, sequenced delivery, and sustained governance.

The difference is not theoretical. It is 803 hours.

WITHOUT OMDDMS®	WITH OMDDMS®
Resilience designed as a compliance exercise	Resilience embedded as a design constraint from the outset
Governance built around attendance, not authority	Governance structured around decision rights and authority
Capability assessed through documentation, not design	Capability gaps identified and sequenced before go-live
Transition managed with a communications plan	Transition designed as an explicit operating model phase
Operating model declared complete at go-live	Operating model governance sustained as a live function
March 2027 treated as a reporting project	March 2027 designed for, not reported against

803 HOURS

That is only one metric of treating operational resilience as a compliance problem rather than an operating model design problem. What about the impact on customers - the time wasted, the fees incurred, the hits to credit ratings through no fault of their own? We rarely hear about that.

In March 2026, the regulator told firms what was wrong. That was three months ago and only 12 months before a new set of requirements comes into force. We all know that project time seems to go into an accelerated dimension.

The question is whether those three months have been spent wisely and productively - because there are only nine months left.

The question is not whether your organisation is exposed. The question is whether you have the methodology to close the gap before March 2027, or whether the next self-assessment will show the same findings as the last one.

SOURCES

1. Treasury Select Committee, 6 March 2025 - More than one month's worth of IT failures at major banks and building societies in the last two years. committees.parliament.uk. Confirms: 803 hours, 158 incidents, nine institutions, Barclays potential £12.5m compensation exposure, Dame Meg Hillier quote.

2. Financial Conduct Authority, 27 March 2026 - Operational Resilience: Insights and Observations One Year On. fca.org.uk. Confirms: six-component review framework covering important business services and impact tolerances, mapping, scenario testing, vulnerability management, communications, and self-assessment quality.

3. FCA PS26/2 / PRA PS7/26 / Bank of England, 18 March 2026 - Operational Incident and Third-Party Reporting. fca.org.uk / bankofengland.co.uk. Confirms: unified reporting regime, 18 March 2027 implementation, 24-hour initial reporting, SMF24 accountability, material third-party register.

4. NatWest Group, letter to the Treasury Select Committee, 26 February 2025. committees.parliament.uk. Confirms: 13 incidents, 194 hours of customer impact, c.142 hours attributable to a single incident.

5. Danske Bank (Northern Bank Limited), letter to the Treasury Select Committee, 26 February 2025. committees.parliament.uk. Confirms: 5 incidents, cumulative duration 113 hours 56 minutes, including a CHAPS-related incident with c.60 hours falling within a scheme-closed weekend period.

6. Barclays Bank UK PLC, letter to the Treasury Select Committee, 26 February 2025 (including annex). committees.parliament.uk. Confirms: 15 channel-impacting incidents, 93 hours total impact, January 2023 - January 2025; excludes the separately reported 31 January - 2 February 2025 incident.

SOURCES

7. Nationwide Building Society, letter to the Treasury Select Committee, 26 February 2025. committees.parliament.uk. Confirms: 18 PSDR 99-reportable incidents, total duration 70 hours 26 minutes, January 2023 - January 2025.

8. Bank of Ireland UK, letter to the Treasury Select Committee, 27 February 2025. committees.parliament.uk. Confirms: five major operational incidents 2023-2024; three with stated durations (c.3, c.7, and c.12 hours); two payment-processing delay incidents without a stated duration; c.£350,000 paid in compensation.

9. Santander UK plc, letter to the Treasury Select Committee, 26 February 2025 (including appendix). committees.parliament.uk. Confirms: 24 channel-availability incidents plus 8 service-level incidents; cumulative per-channel outage time of c.116 hours, reported by channel rather than by incident.