FOURTHLINE

UK Banking Sector
Operational Resilience and Business Continuity
Fourthline Industry Guide

This guide is written for SMF24 holders, Chief Operating Officers, and senior risk and compliance leaders at UK-regulated banks, challengers, and building societies. It sets out what the regulators require, where banking firms typically struggle, and what good looks like from a resilience and business continuity standpoint.

01 THE REGULATORY LANDSCAPE

Banking is the most intensively regulated sub-sector within UK financial services from an operational resilience standpoint. Both the PRA and FCA impose overlapping and, in some areas, reinforcing obligations. For internationally active firms, DORA introduces a further layer.

- PRA SS1/21 and FCA PS21/3 set out the framework for important business service identification, impact tolerance setting, and scenario testing. The March 2025 testing deadline is passed. Scenario testing is now a continuing annual obligation. The PRA has signalled that supervisory engagement will increasingly focus on the quality and severity of scenario test evidence rather than on whether firms have a programme at all.
- FCA SYSC 15A applies to all FCA-regulated credit institutions and imposes specific requirements on ICT risk management, ICT continuity planning, and third-party oversight. For banks with both FCA and PRA authorisation, SYSC 15A obligations sit alongside PRA expectations under SS1/21.
- PRA SS2/21 (Outsourcing and Third Party Risk) sets detailed expectations for the governance, risk management, and oversight of outsourced arrangements. Banking firms are expected to maintain a complete register of material outsourcing arrangements, conduct ongoing supplier risk assessments, and hold documented and tested exit plans for each material arrangement.
- DORA: From January 2025, UK banks with EU-regulated subsidiaries, branches, or group entities caught within DORA scope face direct DORA obligations for those entities, including ICT risk management, incident reporting (72-hour timeline), and TLPT requirements. UK-only banks are not directly subject to DORA but the FCA and PRA have signalled alignment of supervisory expectations.
- FCA PS26/2 introduces mandatory operational incident reporting and material third-party reporting obligations with effect from March 2027. Banking firms should begin implementation planning now, including incident classification frameworks, reporting thresholds, and third-party register alignment with PS26/2 requirements.
- SM&CR: The SMF24 Senior Manager Function carries personal accountability for the resilience governance framework. For banking firms, the complexity of IBS mapping and the volume of material outsourcing arrangements means the SMF24 function requires active programme oversight, not passive sign-off.

02 TYPICAL IMPORTANT BUSINESS SERVICES

For UK banks, important business services are typically anchored around payments, lending, deposit access, and market infrastructure. The specific services depend on firm type: retail, commercial, challenger, or specialist.

Retail and SME Banking	Commercial and Wholesale Banking
Retail Current Account and Deposit Access	Commercial Lending and Facility Management
Card Payments and Contactless Services	Trade Finance and Documentary Credits
Mortgage Origination and Drawdown	FX and Treasury Settlement
Personal and Business Loan Servicing	CHAPS and Faster Payments Processing
Online and Mobile Banking Platform	SME Banking and BCA Services
Branch Banking Operations	Regulatory and Prudential Reporting (COREP, FINREP)

03 WHERE HARM OCCURS: THE IMPACT TOLERANCE VIEW

Banking disruptions translate into harm more rapidly and more visibly than most other financial services sectors. The harm dimensions regulators focus on most closely are:

- Payment system inaccessibility: An inability to access current accounts, make payments, or operate card services creates immediate and severe financial harm for retail customers, particularly those with limited financial resilience. Regulators expect impact tolerances for these services to be very short, often measured in hours rather than days.
- Lending and credit facility disruption: For commercial clients, a failure to process drawdown requests or manage credit facilities can cause cascade failures across supply chains. The harm is systemic as well as individual.
- Consumer Duty obligations: Retail banks carry specific Consumer Duty obligations around product fair value, support for vulnerable customers, and information clarity. A resilience failure that leaves a vulnerable customer unable to access funds or make urgent payments creates a direct Consumer Duty breach alongside the operational failure.
- Market integrity risk: Banks that act as settlement agents, market makers, or provide clearing services carry systemic risk implications. A disruption to settlement or clearing functions can have market-wide consequences and triggers immediate regulatory notification obligations.
- Financial crime and fraud risk: Banking systems outages or degraded monitoring capability create windows of elevated fraud and financial crime exposure. The FCA treats a failure to maintain financial crime controls during an operational disruption as a separate regulatory risk, not merely a consequence of the outage.

04 UNIQUE CHALLENGES FOR INSURANCE FIRMS

Banking firms face a set of operational resilience challenges that differ materially from other regulated sectors. These are not generic technology or process risks. They are structural to the banking model.

- Payment system dependency: UK banks are deeply dependent on third-party payment infrastructure, including Faster Payments, CHAPS, and BACS. A disruption to any of these systems creates an incident that the firm cannot resolve independently, regardless of how strong its internal resilience programme is. Firms must have contingency plans for external payment system outages, not just internal failures.
- Legacy core banking infrastructure: Many mid-tier banks and building societies operate on core banking platforms that are decades old and were not designed for cloud-native resilience architecture. Migration projects are high-risk and multi-year. In the interim, firms must build resilience around legacy constraints, not assume they will be resolved.
- Challenger bank growth risk: Challenger banks and neo-banks face a specific version of this challenge: rapid customer growth outpacing resilience programme maturity. A firm that onboards 500,000 customers in 18 months may be running an important business service at a scale that its BCM programme was never tested against.
- Concentration in cloud and SaaS: UK banking is increasingly concentrated in a small number of cloud providers and core banking SaaS platforms (Temenos, Thought Machine, Mambu, Finastra). A failure at any of these providers could affect multiple regulated banks simultaneously. Firms must have credible fallback positions, not merely contractual SLAs.
- Branch network complexity: Retail banks with physical branch networks face a resilience challenge that digital challengers do not. Branch closures, staff unavailability, and physical access disruption all require specific plans that go beyond ICT recovery. For building societies in particular, branch availability is directly tied to important business service delivery for a significant portion of the customer base.
- Simultaneous regulatory reporting obligations: Banking firms carry overlapping regulatory reporting requirements across COREP, FINREP, Bank of England data collections, and FCA returns. A systems disruption that impairs reporting capability creates a separate regulatory exposure on top of the operational incident itself.

05 CRITICAL RESOURCE DEPENDENCIES

The following represent the most common critical dependencies in banking resilience assessments. These are the points at which third-party failure most directly translates into important business service disruption.

Technology Platforms	Critical Third Parties
Core Banking Platforms (Temenos T24, Thought Machine Vault, Mambu, Finastra Fusion)	Faster Payments, CHAPS, BACS infrastructure
Online and Mobile Banking Front Ends (third-party or in-house)	IT Managed Service Providers and Data Centre Operators
Payment Processing Engines (VocaLink, Mastercard, Visa)	Cloud Hosting Providers (AWS, Azure, Google Cloud)
Fraud and Financial Crime Monitoring Systems (Featurespace, NICE Actimize)	KYC and AML Compliance Utilities (Experian, Refinitiv, LexisNexis)
CRM and Lending Origination Systems (Salesforce, nCino)	Core Outsourced Operations Partners (BPO, print, mail, contact centre)

PRA SS2/21 requires documented and tested exit plans for each material outsourcing arrangement. FourthLine's consistent finding is that banking firms have registers of material outsourcing but exit plans that are either absent, untested, or insufficiently detailed to be operable under stress.

06 THE FOURTHLINE PERSPECTIVE: WHAT GOOD LOOKS LIKE

FourthLine has delivered resilience programmes for UK banking firms across retail, challenger, and specialist segments. The pattern we see consistently is the same: documentation has been completed but testing has not been conducted at a severity level that would reveal whether the programme actually works under stress.

- The firms that perform well under PRA supervisory review can trace a clear evidence chain from IBS identification through impact tolerance setting to scenario design and testing outcome. The evidence is specific to the firm's actual services and dependencies, not generic.
- Banking SMF24 holders are increasingly being asked direct questions about resilience evidence in supervisory meetings. The expectation is that the SMF24 holder can speak to the findings from the firm's most recent scenario test, not merely confirm that a programme exists.
- Supplier exit planning is the area where the largest gap exists in mid-tier banking. Most firms have a list of material outsourcing arrangements. Far fewer have tested whether they could actually execute an exit from their most critical supplier under stressed conditions.
- PS26/2 readiness is becoming an urgent priority. Firms that do not have operational incident classification frameworks, reporting thresholds, and third-party notification processes in place before March 2027 will face a significant implementation sprint under regulatory scrutiny.

The PRA is not asking whether you can document your resilience programme. It is asking whether you have tested it at a level of severity that would tell you whether it works.

07 HOW FOURTHLINE WORKS WITH BANKING FIRMS

FourthLine delivers structured, proportionate resilience programmes for mid-tier UK banks and building societies. Our core services for banking clients include:

- Operational Resilience Diagnostic: A rapid assessment of current programme maturity against SS1/21, SYSC 15A, SS2/21, and PS26/2 requirements. Completed in four to six weeks with a board-ready gap register and remediation roadmap as the primary output.
- BCM Programme Design and Documentation: End-to-end BCM programme delivery, including IBS mapping, impact tolerance setting, BIA, departmental BCRPs, firm-level plan, and SMF24 sign-off support.
- Scenario Testing and Exercising: Design and facilitation of tabletop exercises anchored in banking-specific scenarios. Payment system failure, core banking platform outage, cyber incident affecting operations, and key supplier exit.
- Supplier Exit Planning and Testing: Development of documented exit plans for material outsourcing arrangements and structured exit testing exercises to validate whether plans are operable under stress.
- PS26/2 Implementation Support: Operational incident classification framework, reporting threshold design, third-party register alignment, and regulatory notification process development.
- Annual Resilience Retainer: Ongoing programme maintenance, regulatory intelligence, and SMF24-level assurance support.

START A CONVERSATION

If you are an SMF24, COO, or Head of Risk at a UK-regulated insurer and you want to move from documentation to demonstrable resilience readiness, we would like to talk.

Kieran Maplesden
Founder & Managing Director
Fourthline Ltd
kieran.maplesden@thefourthline.co.uk