FOURTHLINE

FOURTHLINE | CYBER RESILIENCE

Cyber Resilience

A FourthLine Solution Guide for CISOs and Information Security Leaders at UK-Regulated Financial Services Firms

This guide is written for CISOs, Heads of Information Security, and senior technology risk leaders at mid-tier UK financial services firms carrying FCA or PRA operational resilience obligations. It sets out the operating context, regulatory and business drivers, the threat landscape, and how FourthLine's Cyber Resilience Framework module addresses the structural gap most mid-tier firms have between their cybersecurity controls environment and their cyber resilience capability.

01 OPERATING CONTEXT: THE DISTINCTION BETWEEN CYBERSECURITY AND CYBER RESILIENCE

Mid-tier financial services firms have typically invested in cybersecurity controls: firewalls, endpoint detection, patching programmes, access controls, and security awareness training. What most have not built is cyber resilience: the structured, board-governed capability to withstand, respond to, and recover from a significant cyber incident while maintaining important business service delivery.

The distinction matters because the regulator now makes it explicitly. The FCA's operational resilience framework treats cyber incidents as a leading cause of important business service disruption and expects firms to evidence not just that they have preventive controls but that their response and recovery capabilities have been tested at a level of severity that reflects the actual threat landscape.

- Most mid-tier firms have security controls. Far fewer have a documented Cyber Incident Response Plan that is integrated with their crisis management structure and has been tested against a realistic scenario.
- The FCA does not accept a controls audit as evidence of cyber resilience. The question it asks is whether the firm can demonstrate tested capability to respond to and recover from a cyber incident of defined severity within its impact tolerances.
- Ransomware, supply chain compromise, and data breach are no longer low-probability events for FS firms. They are the expected threat profile. A resilience programme that is not built around these scenarios is not fit for regulatory purpose.

02 REGULATORY DRIVERS

Regulatory Framework	Core Obligation
FCA PS21/3 and PRA SS1/21	FCA SYSC 13
Cyber incidents are a named cause of IBS disruption. Scenario testing must include cyber scenarios. Impact tolerances must be tested against cyber-triggered disruption, not just technology failure.	Operational risk management requirements covering information security, cyber risk, and technology risk. Requires documented controls, risk assessments, and evidence of management oversight.

Regulatory Framework	Core Obligation
NCSC Cyber Assessment Framework (CAF)	NIST CSF 2.0
The UK government's primary framework for assessing cyber resilience across critical sectors. FCA supervisory expectations are increasingly CAF-aligned, particularly on governance, risk management, detection, and response.	The updated NIST Cybersecurity Framework provides the Govern, Identify, Protect, Detect, Respond, and Recover architecture that FourthLine uses to organise its cyber resilience programme design.

Regulatory Framework	Core Obligation
FCA PS26/2 (from March 2027)	DORA (EU-facing firms)
Mandatory operational incident reporting including cyber incidents. 72-hour reporting timelines for major incidents. Firms must have cyber incident classification frameworks and regulatory notification procedures embedded before go-live.	ICT risk management and resilience testing requirements for firms with EU-regulated operations. DORA explicitly requires threat-led penetration testing (TLPT) for significant firms and 72-hour major incident reporting.

Regulatory Framework	Core Obligation
UK GDPR / DPA 2018	ISO/IEC 27001:2022
Data breach incidents trigger ICO notification obligations within 72 hours where there is a risk to individuals. Cyber resilience plans must embed ICO notification procedures alongside FCA and PRA reporting.	The primary international standard for information security management. FourthLine's cyber resilience framework is designed to complement and extend an existing ISO 27001 programme rather than duplicate it.

03 BUSINESS DRIVERS

For a CISO at a mid-tier FS firm, the business case for a structured cyber resilience programme extends beyond regulatory compliance. The commercial and operational drivers are significant and increasingly board-visible.

- Cyber insurance requirements: Cyber insurers are progressively requiring evidence of structured incident response capability, tested recovery procedures, and board-level cyber governance as conditions of policy underwriting or premium determination. A firm that cannot evidence these capabilities faces coverage gaps or prohibitive premiums.
- Client and institutional investor scrutiny: Institutional clients, fund investors, and large counterparties routinely conduct cyber due diligence on firms they engage with. A mid-tier FS firm that cannot produce evidence of a structured cyber resilience programme is at a commercial disadvantage in these relationships.
- Ransomware economic reality: The average cost of a ransomware incident for a mid-tier FS firm significantly exceeds the cost of a structured resilience programme. This includes direct recovery costs, regulatory notification costs, potential FCA enforcement, client attrition, and reputational damage. The ROI case for investment is straightforward.
- Board accountability under SM&CR: Named SMF24 holders carry personal accountability for the adequacy of the firm's operational resilience governance, which includes cyber risk. A CISO who cannot present the board with evidence of tested cyber resilience capability is creating personal accountability risk for the SMF24 holder as well as the firm.
- Supply chain expansion of the threat surface: The growth of SaaS, cloud, and AI-tool adoption in mid-tier FS firms has materially expanded the cyber threat surface. Each new third-party platform is a potential entry point. Cyber resilience programmes that do not extend to supply chain cyber due diligence and contractual incident notification obligations are structurally incomplete.

04 THREAT LANDSCAPE: WHAT YOU ARE RECOVERING FROM

Cyber resilience programme design must be grounded in the specific threat landscape relevant to mid-tier UK FS firms. The scenarios that matter most are:

Ransomware and Extortion	Supply Chain and Third-Party Compromise	Insider and Social Engineering
Encryption of primary systems and backups	Managed IT provider as attack vector	Privileged insider access abuse
Exfiltration and double-extortion threat	SaaS platform compromise affecting multiple tenants	Phishing and spear-phishing campaigns
Business email compromise as initial vector	Software supply chain injection	Credential theft and account takeover
Ransomware-as-a-service affiliate campaigns	Cloud provider account compromise	Deepfake-enabled voice or video fraud
Destructive wiper attacks masquerading as ransomware	AI tool data leakage and prompt injection	Impersonation of senior leadership (CFO fraud)

05 THE GAP: WHY CONTROLS ARE NOT SUFFICIENT

The most consistent finding in FourthLine's cyber resilience assessments of mid-tier FS firms is that security controls investment has not been matched by resilience capability investment. The gap manifests in four areas:

- No documented Cyber Incident Response Plan: Many firms have an informal incident response process but lack a documented CIRP that specifies detection triggers, containment procedures, eradication steps, recovery actions, regulatory notification timelines, and communication protocols. Under stress, an undocumented process fails.
- No integration with crisis management: Where a CIRP exists, it often operates independently of the firm's crisis management structure. The Crisis Management Team is not briefed on cyber escalation triggers. SMF accountabilities for cyber incidents are not confirmed. The legal, communications, and regulatory notification workstreams are not pre-planned.
- No tested scenario: Tabletop exercising of cyber scenarios is the exception rather than the norm at mid-tier firms. The vast majority have never tested their leadership team's decision-making under a simulated ransomware or data breach scenario. The FCA expects this to be part of the regular testing programme.
- Supplier cyber due diligence gaps: Most mid-tier firms have not assessed the cyber resilience posture of their material ICT suppliers or embedded cyber incident notification obligations in supplier contracts. A supply chain compromise that is not detected or reported by a supplier within a contractually defined window leaves the firm blind to an active incident.

The FCA's position is clear: preventive controls are necessary but not sufficient. The question it asks in supervisory engagement is whether the firm has tested its ability to respond to and recover from a cyber incident at a level of severity that reflects the real threat.

06 STANDARDS ALIGNMENT: THE FRAMEWORK ARCHITECTURE

FourthLine's Cyber Resilience Framework is built at the intersection of regulatory expectation and international best practice. The methodology references:

- NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover provide the organising architecture. The updated 2024 version of NIST CSF adds the Govern function as the foundational layer, reflecting the importance of board-level accountability and risk management integration that the FCA also emphasises.
- NCSC Cyber Assessment Framework: The CAF's four objectives (Managing Security Risk, Protecting Against Cyber Attack, Detecting Cyber Security Events, Minimising the Impact of Cyber Security Incidents) directly align with FCA supervisory expectations for mid-tier FS firms.
- ISO/IEC 27001/27002:2022: FourthLine's framework is designed to sit alongside and extend an existing ISO 27001 programme. Where a formal ISMS does not exist, the module produces the policy and governance components required to establish one.
- ISO/IEC 27035 (Incident Management): The international standard for information security incident management provides the procedural reference model for CIRP design, including detection, reporting, assessment, response, and lessons learned.
- ISO 22301:2019 and ISO 22361:2022: Business continuity and crisis management standards that provide the BCM and crisis architecture within which the CIRP is integrated. FourthLine ensures that cyber resilience and BCM are not parallel but connected programmes.
- FCA SYSC 15A and PS21/3: All framework components are mapped to specific regulatory obligations to ensure that programme evidence is directly usable in regulatory self-assessment, supervisory review, and the annual resilience self-assessment required under PS21/3.

07 THE FOURTHLINE TECHNOLOGY RESILIENCE FRAMEWORK

FourthLine's Cyber Resilience Framework is structured across six domains aligned to NIST CSF 2.0 and NCSC CAF principles. The framework bridges cybersecurity controls and operational resilience, positioning cyber risk as a board-governed resilience discipline rather than a standalone IT function.

GOVERNANCE	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Executive Buy-in	Scope Definition	Identity Asset Mgmt (IAM)	SIEM	Business Continuity Recovery Plan	System Restoration from Backup
Roles and Responsibilities	Business Impact Analysis	Data Encryption	Endpoint Detection (EDR)	Incident Response Plan	BCM/DR/Technology Playbooks
Cyber Resilience Status	Security Impact Analysis	Data Loss Prevention (DLP)	Network Monitoring	Containment and Eradication	Lessons Learned
KRI / KPI Reporting	Minimum Viable Business	Security Patching	Detection Tools	Crisis Management	DR Backup and Recovery Tools
Policies and Standards	Crown Jewels / Critical Assets	Training and Awareness		Crisis Communication	DR and Data Recovery Testing
	Critical Service Mapping (CMDB)	Protection Tools		Cyber Forensics	

The framework is underpinned by two horizontal layers that run across all six domains: Framework Documentation (NIST 2.0 controls, playbooks, CIRPs, BIAs, CMABDs, TPRM cyber due diligence) and Exercising and Testing (scenario desktop exercises, red/blue/purple team testing, auditing, control testing, data recovery testing, and third-party testing).

08 FOURTHLINE'S APPROACH: THE CYBER RESILIENCE MODULE

The Cyber Resilience module is designed for firms that have cyber security controls in place but lack a structured resilience framework, defined incident response capability, tested recovery procedures, or a credible board-level reporting architecture for cyber risk.

Phase 1: Baseline and Risk Integration	Phase 2: CIRP and CMT Integration	Phase 3: Exercising and Board Reporting
Cyber Resilience Baseline Assessment	Cyber Incident Response Plan (CIRP) development	Cyber tabletop exercise facilitation
Assessment across five domains: governance, threat/risk, protective controls, detection, response/recovery	Coverage: detection, containment, eradication, recovery	Scenario calibrated to firm threat profile
Aligned to NCSC CAF and NIST CSF 2.0	Scenario coverage: ransomware, data breach, third-party compromise, insider threat	Leadership-level decision-making exercise
Scored baseline with prioritised gap register	Integration with Crisis Management Team escalation framework	Regulatory notification judgement tested
Cyber risk taxonomy and appetite statements	SMF accountability mapping for cyber incidents	Post-exercise action log and improvement plan
Integration with enterprise risk register	FCA, ICO, and PRA notification timelines embedded	Board cyber resilience dashboard and reporting template
Cyber risk reporting structure to board risk committee	Supplier cyber resilience assessment for critical ICT third parties	KRI, testing status, incident metrics, regulatory horizon
		Cyber Resilience Improvement Roadmap for Year 2

09 DELIVERABLES

Deliverable	Deliverable
Cyber Resilience Baseline Assessment Report with scored gap register	Supplier Cyber Resilience Assessment covering critical ICT third parties
Cyber Risk Register and risk appetite statement aligned to IBS impact tolerances	Cyber Tabletop Exercise: scenario design, facilitation, and post-exercise action plan
Cyber Incident Response Plan (CIRP) integrated with CMT and BCM framework	Board Cyber Resilience Reporting Template and initial population
SMF accountability map for cyber incident response and regulatory notification	Cyber Resilience Improvement Roadmap for the Year 2 testing cycle

10 INTEGRATION WITH OPERATIONAL RESILIENCE AND RELATED PROGRAMMES

FourthLine designs all cyber resilience work to integrate directly with the firm's wider operational resilience architecture, not to operate as a parallel and disconnected programme.

- Operational Resilience and IBS: Cyber risk is assessed at the IBS level. Impact tolerances for each IBS are the reference point for CIRP recovery objectives. The scenario testing programme includes cyber-triggered IBS disruption scenarios alongside technology failure and operational scenarios.
- BCM Programme: The CIRP is integrated with departmental BCRPs and the Organisational Crisis Management Plan. BCP activation triggers include cyber incident escalation thresholds. The BCM testing cycle incorporates cyber scenarios alongside non-cyber disruption events.
- ICT Resilience and Service Continuity: Cyber incidents are among the most likely triggers for ICT service continuity events. The CIRP and ITDR procedures share the CMT escalation architecture and are designed to be activated in parallel where a cyber incident triggers a recovery requirement.
- Third Party Risk Management: Supplier cyber resilience due diligence, contractual incident notification obligations, and supply chain cyber scenarios are coordinated with the TPRM programme. Critical ICT third parties are assessed for cyber resilience as part of the ongoing supplier oversight cycle.
- Regulatory Reporting (PS26/2 and ICO): Cyber incident classification frameworks, reporting thresholds, and notification procedures produced by the module are designed to satisfy both the FCA PS26/2 obligations from March 2027 and the ICO 72-hour notification requirement under UK GDPR.

START WITH A DIAGNOSTIC

FourthLine's Cyber Resilience Diagnostic assesses your current posture across the five domains of governance, threat and risk management, protective controls, detection and monitoring, and response and recovery. Completed in four to six weeks. Output: a scored baseline, prioritised gap register, and board-ready remediation roadmap.

If you are a CISO, Head of Information Security, or SMF24 holder at a UK-regulated financial services firm and you want to understand the gap between your current cyber controls environment and a structured, tested, board-governed cyber resilience capability, the right first step is a structured diagnostic.

www.thefourthline.co.uk | kieran.maplesden@thefourthline.co.uk