FOURTHLINE

FOURTHLINE | TECHNOLOGY RESILIENCE

ICT Resilience and Service Continuity

A FourthLine Solution Guide for CTOs and Technology Risk Leaders at UK-Regulated Financial Services Firms

This guide is written for CTOs, Heads of Technology Risk, and IT Directors 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 technical challenges in meeting recovery objectives, and how FourthLine's ICT Resilience and Service Continuity module addresses them.

01 OPERATING CONTEXT: WHY ICT RESILIENCE IS A BOARD-LEVEL ISSUE

Mid-tier financial services firms increasingly operate in a technology environment characterised by deep cloud dependency, multi-layer outsourcing, and a legacy infrastructure base that was not designed for the recovery standards regulators now require. The combination of these factors creates a structural gap between what firms believe their recovery capability to be and what it demonstrably is when tested.

Three operating realities define the challenge:

- The IBS obligation has materialised: Since the March 2025 deadline under PRA SS1/21 and FCA PS21/3, firms are required to demonstrate, through scenario testing, that they can remain within their impact tolerances. Impact tolerances are defined at the business service level. Technology recovery capability must therefore be evidenced in direct relation to business service recovery, not system availability in isolation.
- The regulatory lens has shifted from documentation to evidence: Regulators are no longer satisfied by a written DR plan. The question in PRA supervisory meetings is whether that plan has been tested at a severity that would reveal whether the RTOs and RPOs it specifies are actually achievable. Most mid-tier firms cannot answer that question confidently.
- Technology dependency is the most common root cause of IBS failure: Across FourthLine's engagement base, ICT failure or degraded ICT capability is the most frequently cited root cause of important business service disruption. Firms with strong BCM documentation but weak ICT service continuity capability have a resilience programme that is built on an untested foundation.

02 REGULATORY DRIVERS

Regulatory Framework	Core Obligation
FCA SYSC 15A	PRA SS1/21 / FCA PS21/3
Specific ICT business continuity and ICT risk management requirements for MiFID and AIFMD firms. Requires documented ICT continuity plans, regular testing, and third-party ICT oversight.	Important business services must remain within impact tolerances through severe but plausible disruption. Technology recovery capability must be calibrated to business impact tolerances, not IT preference.

Regulatory Framework	Core Obligation
ISO/IEC 27031:2011	PRA SS2/21
The primary international standard for ICT readiness for business continuity. Defines the programme components, testing requirements, and governance expectations for ICT service continuity.	Material outsourcing arrangements must have documented and tested exit plans. Firms relying on cloud or managed IT providers for critical systems must evidence recovery capability independent of those providers.

Regulatory Framework	Core Obligation
FCA PS26/2 (from March 2027)	DORA (EU-facing firms)
Mandatory operational incident reporting and material third-party reporting. ICT incident classification and reporting timelines must be embedded in the ICT resilience framework before go-live.	ICT risk management, 72-hour major incident reporting, and TLPT requirements for firms with EU-regulated entities or operations caught within scope.

03 BUSINESS DRIVERS

Beyond regulatory compliance, CTOs at mid-tier firms face a set of practical business pressures that make a structured ICT resilience programme a commercial necessity rather than a compliance overhead.

- Customer and client retention: A platform or trading system outage that prevents clients from accessing services creates immediate reputational harm, client attrition risk, and, for Consumer Duty firms, a direct regulatory exposure. The commercial cost of a visible outage routinely exceeds the cost of the resilience programme that could have prevented it.
- Operational efficiency: Firms that invest in resilience by design, including high availability architecture, automated failover, and observable systems, consistently achieve lower incident frequency and faster mean time to recovery compared to firms relying solely on reactive DR procedures.
- Board and audit confidence: The board and audit committee increasingly require technology risk reporting that goes beyond infrastructure health metrics. Evidence of tested recovery capability against business-defined RTOs and RPOs is the standard of assurance now expected at senior governance level.
- Supplier contract leverage: Firms with clearly documented RTOs, RPOs, and recovery test requirements are in a materially stronger position when negotiating SLAs, contractual resilience standards, and incident notification obligations with cloud and managed service providers.
- M&A and due diligence readiness: ICT service continuity capability is a standard diligence item in acquisition and investment transactions involving regulated FS firms. Gaps in this area create valuation risk and can delay or complicate transaction timelines.

04 THREAT LANDSCAPE: WHAT YOU ARE RECOVERING FROM

An ICT resilience programme that is not grounded in the specific threat landscape of the firm is unlikely to be credible under regulatory or operational scrutiny. The scenarios that mid-tier FS firms most commonly need to recover from are:

Technology Failure Scenarios	Cyber-Triggered Recovery Scenarios	Compound and External Scenarios
Cloud provider regional outage	Ransomware encryption of primary systems	Simultaneous cloud and network failure
Core banking or platform system failure	Data breach triggering system isolation	Supplier failure coinciding with market stress
Managed IT provider failure	Destructive malware or wiper attack	Physical facility loss combined with IT disruption
Database corruption or data integrity failure	Supply chain compromise affecting critical platform	Key person unavailability across technology function
Network or connectivity loss	Insider threat with system access	Regulatory-driven system suspension
Data centre or co-location facility failure	DDoS attack on customer-facing infrastructure	Third-party platform withdrawal or insolvency

05 THE TECHNICAL CHALLENGE: MEETING RTOS AND RPOS UNDER STRESS

The most common gap FourthLine identifies in mid-tier firm ICT resilience assessments is not the absence of a DR plan. It is the absence of verified alignment between the RTOs and RPOs stated in the plan and the firm's actual technical recovery capability. This gap has four principal causes:

- RTO and RPO set by IT, not business: Where recovery objectives are established by the technology function in isolation, they typically reflect what is technically achievable rather than what the business requires to remain within its impact tolerances. An RTO of 24 hours may be technically achievable. If the firm's impact tolerance for its core payment service is four hours, the plan fails at the first test of regulatory relevance.
- Backup and replication coverage gaps: Most mid-tier firms have backup processes in place. Fewer have verified that backup coverage extends to every ICT asset supporting an IBS, that backup frequency aligns to RPO requirements, and that restores have been tested end-to-end from backup to operational state at the required tier of criticality.
- Cloud resilience misunderstood as cloud provider resilience: A significant proportion of mid-tier firms conflate their cloud provider's availability SLA with their own recovery capability. A cloud provider maintaining 99.9% uptime does not mean the firm can recover a corrupted or compromised application workload within its RTO. Application-level recovery capability must be separately designed, documented, and tested.
- Runbook quality and personnel dependency: Many DR runbooks are written at a high level of abstraction and depend on institutional knowledge held by specific individuals. Under incident conditions involving staff unavailability, an underdeveloped runbook that requires the author to execute it is not a credible recovery procedure.

The gap between documented RTOs and evidenced recovery capability is the single most consistent finding in FourthLine's ICT resilience assessments. Closing that gap is the core purpose of the module.

06 STANDARDS ALIGNMENT: THE FRAMEWORK ARCHITECTURE

FourthLine's ICT resilience methodology is built on the intersection of regulatory expectation and international best practice standards. The framework architecture references the following:

- ISO/IEC 27031:2011 (ICT Readiness for Business Continuity): The foundational standard for ICT service continuity. Defines the PDCA-based programme lifecycle, recovery objective setting, testing requirements, and the relationship between ICT continuity and the broader BCM programme under ISO 22301.
- ISO 22301:2019 (Business Continuity Management): The overarching BCM standard within which ICT service continuity is embedded. FourthLine's methodology ensures that ICT recovery objectives are derived from and aligned to the business continuity requirements defined under this standard.
- NIST CSF 2.0 (Cybersecurity Framework): The Identify, Protect, Detect, Respond, and Recover functions of NIST CSF provide the organising architecture for FourthLine's technology resilience framework. Recover, in particular, provides the capability reference model for DR programme design and testing.
- ISO/IEC 27001/27002:2022 (Information Security Management): Controls relevant to backup management, access control, change management, and incident response are incorporated into the ICT resilience programme design, ensuring alignment with the firm's information security management posture.
- FCA SYSC 15A and PRA SS1/21: All methodology components are mapped to specific regulatory obligations, ensuring that the evidence produced by the programme is directly usable in regulatory self-assessment and supervisory review.

07 THE FOURTHLINE TECHNOLOGY RESILIENCE FRAMEWORK

FourthLine's technology resilience framework organises capability across five lifecycle phases. The ICT Resilience and Service Continuity module operates primarily across the Identify, Prepare, and Recover phases, with integration into Respond and Adapt through the broader BCM and crisis management architecture.

IDENTIFY	PREPARE	RESPOND	ADAPT	RECOVER
ICT Asset Scope	Architecture Resilience by Design	Incident Management Framework	Lessons Learned Procedure	Recovery Strategies
IBS-to-ICT Mapping	RTO/RPO Calibration to IBS	DR Plans and Procedures	Root Cause Analysis	Data Recovery Procedures
ICT Dependency Mapping	Preventative Controls	Monitoring and Observability	Threat Horizon Scanning	Recovery Validation Testing
ICT Risk Assessment	Testing and Exercising	Internal and External Comms	Change Management	BCM/DR Playbook Integration
Roles and Responsibilities	Awareness and Training	ICT Third Party Oversight	Regulatory Notification	Corporate Culture and Learning

The framework is not a standalone ICT programme. It is designed to sit within the firm's operational resilience architecture, with IBS-to-ICT dependency mapping providing the direct linkage between business continuity obligations and technology recovery capability.

08 FOURTHLINE'S APPROACH: THE ICT RESILIENCE MODULE

The ICT Resilience and Service Continuity module is sequenced after BCM programme completion. The IBS-to-technology dependency mapping produced in the BCM phase provides the direct input to the ITDR scoping exercise, ensuring recovery objectives are anchored to business impact, not IT preference.

Phase 1: Baseline and Mapping	Phase 2: RTO/RPO and Gap Assessment	Phase 3: Recovery Procedures and Testing
ICT Asset and Dependency Baseline	RTO and RPO definition per ICT asset	Recovery runbook development for priority assets
Four-layer workshop: infrastructure, platforms, applications, end-user tech	Calibration to business impact tolerances	Operationally executable under incident conditions
ICT Service Catalogue with recovery tier classification	DR Architecture Review	ITDR tabletop exercise facilitation
Mapping to IBS and hosting model	Backup and replication configuration review	Walkthrough testing of recovery procedures
Gap identification in existing asset register	Failover and fallback capability assessment	Post-exercise action log and improvement plan
	DR Gap Register with remediation recommendations	Board-ready ITDR programme summary

09 DELIVERABLES

Deliverable	Deliverable
ICT Service Catalogue mapped to IBS and recovery tiers	ITDR Tabletop Exercise: scenario design, facilitation, and post-exercise report
RTO and RPO register calibrated to IBS impact tolerances	ITDR integration schedule mapping to BCRPs and Crisis Management Plan
DR Gap Assessment Report with prioritised remediation	Board-ready ITDR programme summary for resilience self-assessment
Recovery runbooks for priority ICT assets (minimum top tier per IBS)	Remediation roadmap across 0-3, 3-12, and 12-24 month horizons

10 INTEGRATION WITH OPERATIONAL RESILIENCE AND RELATED PROGRAMMES

The ICT Resilience module does not operate in isolation. FourthLine designs all technology resilience work to integrate with the firm's broader protective framework:

- BCM Programme: IBS mapping produced in the BCM programme is the direct input to the ICT dependency baseline. ITDR procedures are integrated with departmental BCRPs and the Organisational Crisis Management Plan. Escalation triggers from BCRPs into ITDR procedures are documented and role-assigned.
- Cyber Resilience: ICT recovery capability and cyber incident response are complementary but distinct. The ITDR module addresses recovery from cyber-triggered failures. The Cyber Resilience module addresses the detection, containment, and eradication procedures that precede recovery. Both modules share the Crisis Management Team escalation architecture.
- Third Party Risk Management: Where recovery capability depends on third-party platforms, the ICT module coordinates with TPRM to ensure that supplier resilience standards, contractual SLAs, and exit plan provisions are aligned with the firm's documented RTOs and RPOs.
- Operational Resilience Governance: ITDR test results are reported through the firm's Operational Resilience Steering Group. The board-ready programme summary produced by the module is designed for use in the firm's annual resilience self-assessment and regulatory evidence pack.

START WITH A DIAGNOSTIC

FourthLine's ICT Resilience Diagnostic assesses your current recovery capability across asset coverage, RTO/RPO calibration, backup and replication configuration, runbook quality, and testing evidence. Completed in four to six weeks. Output: a board-ready gap register and remediation roadmap.

If you are a CTO, Head of Technology Risk, or IT Director at a UK-regulated financial services firm and you want to know whether your ICT recovery capability is aligned to your business impact tolerances, the right first step is a structured diagnostic.

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