OPERATIONAL RESILIENCE REQUIREMENTS FOR BANKING INSTITUTIONS

Regulatory Authority: Financial Conduct Authority (FCA) & Prudential Regulation Authority (PRA)

Reference: Policy Statement PS21/3

Effective Date: 31 March 2025

Jurisdiction: United Kingdom

1. INTRODUCTION AND SCOPE

1.1 Purpose

This regulation establishes comprehensive operational resilience requirements for banking institutions to ensure they can prevent, adapt, respond to, recover, and learn from operational disruptions.

1.2 Scope of Application

This regulation applies to:

• All UK-authorized banks and building societies

• Investment firms classified as significant IFPRU firms

• Credit unions with assets exceeding £1 billion

• Branches of foreign banks operating in the UK with deposits exceeding £500 million

2. DEFINITIONS

Important Business Services (IBS): Services provided by a firm that, if disrupted, could pose a risk to the firm's safety and soundness, cause harm to consumers, or impact market integrity.

Impact Tolerance: The maximum tolerable level of disruption to an important business service, defined in terms of the duration of disruption and/or level of degradation.

Severe but Plausible Scenario: A hypothetical event or sequence of events that could cause disruption but is within the bounds of possibility given the firm's risk profile.

Operational Resilience: The ability of firms to prevent, adapt, respond to, recover and learn from operational disruptions.

3. CORE REGULATORY REQUIREMENTS

3.1 Identification of Important Business Services

Requirement 3.1.1: Firms must identify and document all Important Business Services by:

• Conducting comprehensive business impact analysis

• Assessing services against consumer harm criteria

• Evaluating market integrity implications

• Considering safety and soundness impacts

Requirement 3.1.2: The identification process must be reviewed at least annually and whenever there are material changes to business operations.

3.2 Setting Impact Tolerances

Requirement 3.2.1: For each Important Business Service, firms must:

• Set clear, measurable impact tolerances expressed in time-based metrics

• Define acceptable levels of service degradation

• Document the methodology and assumptions used

• Obtain Board approval for all impact tolerances

Requirement 3.2.2: Impact tolerances must be:

• Based on potential consumer harm

• Aligned with regulatory expectations

• Achievable within available recovery capabilities

• Set at a level that prevents intolerable harm

3.3 Scenario Testing

Requirement 3.3.1: Firms must conduct scenario testing at least annually to:

• Test the ability to remain within impact tolerances

• Identify vulnerabilities in operational resilience

• Validate recovery procedures and capabilities

• Test coordination across internal and external dependencies

Requirement 3.3.2: Scenario testing must include:

• At least three severe but plausible scenarios per Important Business Service

• Scenarios involving third-party and critical service provider failures

• Cyber attack scenarios affecting critical systems

• Scenarios combining multiple simultaneous disruptions

3.4 Mapping of Resources and Dependencies

Requirement 3.4.1: Firms must create and maintain detailed mapping of:

• People, processes, technology, facilities, and information supporting each IBS

• Critical third parties and service providers

• Interconnections between business services

• Single points of failure

Requirement 3.4.2: Mapping must be updated:

• At least quarterly

• Within 30 days of any material change

• Following any operational disruption

• As part of any major system or process change

3.5 Third-Party Risk Management

Requirement 3.5.1: Firms must:

• Maintain a register of all third-party service providers

• Assess criticality of each provider to Important Business Services

• Conduct due diligence on providers supporting IBS

• Include operational resilience requirements in contracts

Requirement 3.5.2: For critical third parties, firms must:

• Establish clear SLAs aligned with impact tolerances

• Require evidence of the third party's own resilience capabilities

• Maintain the right to audit third-party controls

• Develop contingency plans for third-party failure

3.6 Communication and Governance

Requirement 3.6.1: Firms must:

• Designate a Senior Manager accountable for operational resilience

• Establish a governance structure with clear roles and responsibilities

• Provide regular Board reporting on resilience capabilities

• Create escalation procedures for tolerance breaches

Requirement 3.6.2: Communication requirements include:

• Notifying the FCA within 4 hours of any breach of impact tolerance

• Providing root cause analysis within 14 days of material disruptions

• Publishing annual operational resilience self-assessment

• Maintaining incident logs accessible for regulatory review

3.7 Documentation and Records

Requirement 3.7.1: Firms must maintain comprehensive documentation including:

• Complete IBS identification methodology and results

• Impact tolerance setting rationale and Board approval minutes

• Scenario testing plans, execution records, and findings

• Mapping documentation with version control

• Third-party assessment records

• Lessons learned from disruptions and near-misses

Requirement 3.7.2: All records must be:

• Retained for a minimum of 7 years

• Made available to regulators within 48 hours of request

• Stored securely with appropriate access controls

• Backed up and recoverable within impact tolerances

4. IMPLEMENTATION REQUIREMENTS

4.1 Implementation Timeline

Phase 1 (By 31 March 2024):

• Complete identification of Important Business Services

• Set impact tolerances for all IBS

• Establish governance framework

Phase 2 (By 30 September 2024):

• Complete initial mapping of resources and dependencies

• Conduct first round of scenario testing

• Implement enhanced third-party risk management

Phase 3 (By 31 March 2025 - Full Compliance):

• Demonstrate ability to remain within impact tolerances

• Complete all documentation requirements

• Implement monitoring and continuous improvement processes

4.2 Submission Requirements

Firms must submit to the FCA and PRA:

• Self-assessment against requirements (by 31 March 2025)

• Annual operational resilience report (within 4 months of financial year-end)

• Material changes to IBS or impact tolerances (within 30 days of change)

5. SUPERVISORY EXPECTATIONS

5.1 Regulatory Assessment

Regulators will assess:

• Completeness and quality of IBS identification

• Appropriateness of impact tolerances

• Effectiveness of scenario testing

• Adequacy of governance and oversight

• Quality of third-party management

5.2 Desk-Based and On-Site Reviews

Firms should expect:

• Annual desk-based reviews of submissions

• On-site inspections focusing on high-risk areas

• Thematic reviews across multiple firms

• Testing of incident response capabilities

6. ENFORCEMENT AND PENALTIES

6.1 Regulatory Powers

The FCA and PRA may exercise the following powers for non-compliance:

Supervisory Actions:

• Requiring additional reporting

• Imposing restrictions on business activities

• Requiring remediation plans with specified timelines

• Appointing skilled persons to review controls

Enforcement Actions:

• Public censure of the firm or individuals

• Financial penalties up to:

• £50 million or 10% of relevant turnover (whichever is higher) for firms

• £1 million or up to 25% of total annual income for individuals

• Prohibition of individuals from performing regulated functions

• Variation or cancellation of regulatory permissions

6.2 Aggravating Factors

Penalties may be increased for:

• Deliberate or reckless breaches

• Failure to cooperate with regulators

• Previous compliance failures

• Actual consumer harm resulting from non-compliance

• Concealment of breaches

7. SPECIFIC REQUIREMENTS BY INSTITUTION TYPE

7.1 Retail Banks

Must prioritize resilience for:

• Payment services (within 2-hour impact tolerance)

• Customer account access (within 4-hour impact tolerance)

• ATM and branch services (within 24-hour impact tolerance)

• Mortgage and lending services (within 48-hour impact tolerance)

7.2 Investment Banks

Must prioritize resilience for:

• Trading platforms and market access (within 15-minute impact tolerance)

• Settlement and clearing services (within 2-hour impact tolerance)

• Client reporting and custody services (within 24-hour impact tolerance)

• Risk management systems (within 1-hour impact tolerance)

7.3 Building Societies

Must prioritize resilience for:

• Member account access and transactions (within 4-hour impact tolerance)

• Mortgage origination and servicing (within 48-hour impact tolerance)

• Savings account services (within 24-hour impact tolerance)

8. TRANSITION PROVISIONS

8.1 Grandfathering

Existing business continuity and disaster recovery plans may be recognized if:

• They meet or exceed new requirements

• They are mapped to the new framework within 6 months

• They include all required documentation

8.2 Proportionality

Smaller firms (assets under £5 billion) may apply proportionality to:

• Scenario testing frequency (minimum annually instead of twice-yearly)

• Documentation requirements (simplified templates permitted)

• Board reporting (semi-annual instead of quarterly)

Proportionality does NOT apply to:

• IBS identification

• Impact tolerance setting

• Notification requirements

• Record retention

9. INTERNATIONAL COORDINATION

9.1 Cross-Border Considerations

Firms operating internationally must:

• Coordinate operational resilience across jurisdictions

• Ensure consistency with host country requirements

• Establish clear recovery protocols for cross-border services

• Document inter-jurisdictional dependencies

9.2 Alignment with International Standards

This regulation aligns with:

• Basel Committee on Banking Supervision principles on operational resilience

• EU Digital Operational Resilience Act (DORA) where applicable

• Financial Stability Board guidance on third-party dependencies

10. REGULATORY CONTACT AND SUPPORT

10.1 Queries and Clarifications

Technical queries should be directed to:

• Email: operationalresilience@fca.org.uk

• Phone: +44 (0)20 7066 1000

• Dedicated portal: https://www.fca.org.uk/operational-resilience

10.2 Industry Guidance

The FCA and PRA will provide:

• Quarterly industry roundtables

• Published case studies and good practice examples

• Thematic feedback statements

• Dedicated supervision teams for major firms

APPENDIX A: IMPACT TOLERANCE SETTING GUIDANCE

When setting impact tolerances, firms should consider:

1. **Consumer Harm Threshold**

• Financial loss to customers

• Loss of access to essential services

• Data security and privacy impacts

• Vulnerable customer considerations

2. **Market Integrity**

• Ability to meet settlement obligations

• Market confidence and functioning

• Information asymmetry risks

3. **Safety and Soundness**

• Regulatory capital impacts

• Liquidity considerations

• Reputational damage

• Competitive position

4. **Technical Feasibility**

• Recovery time objectives (RTO)

• Recovery point objectives (RPO)

• Resource availability

• Third-party dependencies

APPENDIX B: SCENARIO TESTING EXAMPLES

Scenario 1: Cyber Attack on Core Banking System

- Primary system unavailable for 72 hours
- Customer data potentially compromised
- Payment processing severely limited
- Media and reputational impact

Scenario 2: Critical Third-Party Cloud Provider Failure

- All cloud-hosted services unavailable
- Recovery requires activation of alternate provider
- Data restoration from backups required
- Multiple business services affected simultaneously

Scenario 3: Widespread Power Outage

- All primary data centers offline
- Telecommunications infrastructure degraded
- Staff unable to access physical locations
- Duration: 48-96 hours

DOCUMENT CONTROL

Version: 1.0

Publication Date: 15 March 2023

Effective Date: 31 March 2025

Next Review: March 2026

Document Owner: Joint FCA/PRA Policy Team

Classification: Public

END OF REGULATORY DOCUMENT