KPMG

CBI Perspective on Operational Resilience

December 2021

Your Partner For What's Next

Overview and Context

Strengthening resilience throughout the financial system is one of the strategic commitments by the Central Bank of Ireland (CBI). Resilience includes understanding existing vulnerabilities and mitigating those risks to ensure the financial system can withstand and limit the impact of future disruptions. A firm that is operationally resilient can recover its critical or important business services from a significant unplanned disruption, while minimising impact and protecting its customers and the integrity of the financial system.

The first step in becoming operationally resilient is accepting that disruptive events will occur, and that these events will need to be managed effectively. A firm needs to have forward looking plans and can be applied across a range of potential disruptions. A firm should proactively prepare to withstand and adapt to disruptions that will inevitably occur.

The Cross Industry Guidance on Operational Resilience

The Cross Industry Guidance on Operational Resilience sets out a holistic approach to the management of operational resilience and related risks which is built around the following three pillars of Operational Resilience:

- Identify & Prepare
- Respond & Adapt
- Recover & Learn

The three pillars are supported by 15 guidelines which have been developed by the Central Bank following engagement with their international regulatory colleagues. The expectation from the Central Bank is that regulated firms' boards and senior management should take appropriate action to ensure that their operational resilience frameworks are well designed, are operating effectively, and are sufficiently robust Boards should also be able to demonstrate that they have applied the guidelines within an appropriate timeframe, and in a flexible and proportionate manner based on the nature, scale and complexity of the business.

Operational Resilience

Identify & Prepare

1. The Board has ultimate responsibility for the Operational Resilience of a firm.
2. The Operational Resilience Framework should be embedded within a firm's overall Governance and Risk Management Frameworks.
3. The Board review and approve the criteria for critical or important business services.
4. A firm should identify its critical or important business services.
5. Impact tolerances should be approved for each critical or important business service.
6. A firm should develop clear impact tolerance metrics.
7. A firm should understand and map out how its critical or important business services are delivered.
8. A firm should capture third party dependencies in the mapping of critical and important business services.
9. A firm should have ICT and Cyber Resilience strategies that are integral to the operational resilience of its critical or important business services.
10. A firm should document and test its ability to remain within impact tolerances through severe but plausible scenarios.

Respond & Adapt

11. Business Continuity Management should be fully integrated into the overarching Operational Resilience Framework and linked to a firm's risk appetite.
12. The Incident Management Strategy should be fully integrated into the overarching Operational Resilience Framework.
13. Internal and External Crisis Communication plans should be fully integrated into the overarching Operational Resilience Framework.

Recover & Learn

14. A lessons learned exercise should be conducted after a disruption to a critical or important business service to enhance a firm's capabilities to adapt and respond to future operational events.
15. A firm should promote an effective culture of learning and continuous improvement as operational resilience evolves.

"In a world where organisations are faced with complex Technology, Cyber, Data and Third Party challenges, enhancing your firms Operational Resilience is rapidly becoming a strategic priority"

Head of Management Consulting, KPMG Ireland
- Owen Lewis,

The Global Landscape

The Operational Resilience concept has been gaining traction globally and **financial services firms have experienced challenges from various disruptive events including technology failures, cyber incidents, the COVID-19 pandemic and natural disasters**. New standards and consultations are continually being proposed across multiple jurisdictions. While the various authorities might promote different terms, the core aspects remain the same - regulatory authorities are concerned with ensuring a firm can evidence their approach to operational continuity.

The Central Bank confirms that this Guidance is in line with international best practice and compatible with and complementary to the 'Digital Operational Resilience Act' DORA. The Central Bank will continue to update and align the intended outcomes of the supervisory approach with relevant international operational resilience policy developments as they evolve. The Central Bank has determined that there are no contradictions between this Guidance and the forthcoming DORA regulation. There are however, many elements of DORA that, when applied, will require firms to build greater resilience into their critical or important business service and thus align with the intended outcome of these guidelines. The Central Bank confirms that it will continue to monitor international developments after the issuance of this Guidance, including any updates to ICT & Cyber Resilience best practices.

Some examples of relevant guidance are detailed below.

Relevant Marketplace Movements

- The Basel Committee on Banking Supervision's (BCBS) 'Principles for operational resilience';
- The joint Bank of England (BoE), Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) policy statement on their approach to operational resilience across the financial services sector;
- European Commission published its proposed legislation in digital operational resilience, DORA;
- The US Federal Reserve Board (FRB), the UK's PRA, and the European Central Bank (ECB) have agreed coordinated statements on operational resilience, which have been issued to all Global Systemically Important Banks (GSIBs), and non-GSIBs;
- The UK has taken the lead in developing the concept of Operational Resilience, with other jurisdictions paying close attention. It is expected that, over time, a global approach will emerge. Operational Resilience is the new consideration all financial services firms will have to adapt to going forward.

Timing & Expectations

The CBI has released the Cross Industry Guidance on Operational Resilience in December 2021. The authority expects firms to actively and promptly address their operational resilience vulnerabilities and be in a position to evidence actions / plans to apply the guidance by the end of 2023.

The Central Bank will conduct supervisory engagements to assess the level of Operational Resilience maturity in firms. This includes looking for evidence that the board is seeking the required information to enable it to understand the risk and resilience profile of the firm, the firm's understanding of the delivery of its own critical or important business services and the operational assets that underpin the delivery of these services, the firm's ability to determine appropriate impact tolerances for its important business services and the firm's consideration of third parties in its response and recovery process.

How KPMG can help

KPMG has supported clients on their Operational Resilience journeys since 2017 and has extensive experience in Ireland, the UK and Europe via our Operational Resilience Centre of Excellence. Specifically, our team has deep technical expertise across the Operational Resilience Pillars as outlined by the CBI including ICT and Cyber Resilience, Incident Management, and Business Continuity in addition to broad governance risk, regulatory and compliance skills.

KPMG can help you with…

- **Strategy –** Defining the business case for Operational Resilience and defining strategic priorities.
- **Maturity Assessment –** Determining the level of your firm's operational resilience maturity.
- **Programme Assurance –** Assessment of your Operational Resilience Programme to ensure compliance.
- **Operating Model Design –** Developing the Op Model for your Operational Resilience. Business Unit and wider organisation.
- **Implementation Roadmap –** Operational Resilience implementation plan and roadmap to compliance.
- **Important Business Service Governance –** Defining your firm's Important Business Services and sign-off.
- **Scenario Testing & Impact Tolerances –** Conducting simulations and developing resultant Impact Tolerances.
- **Data & Tooling –** Assessment of your functional data & tooling requirements for Operational Resilience.

Contact Us

Owen Lewis
Partner & Head of Management Consulting in KPMG Ireland
T: +353 87 050 4760
E: owen.lewis@kpmg.ie

Ian Nelson
Partner & Head of Regulatory, Head of Banking & Capital Markets
T: +353 87 744 1989
E: ian.nelson@kpmg.ie

Patrick Farrell
Partner Risk Consulting
T: +353 87 050 4029
E: Patrick.farrell@kpmg.ie

David Polley
Director, Management Consulting, Regulatory Driven Transformation. T: +353 87 111 5970
E: david.polley@kpmg.ie

Ashley Harris
Director, Financial Services at KPMG UK, Operational Resilience Lead
T: +44 (0)7775 817 534
E: ashley.harris@kpmg.co.uk

kpmg.ie

Produced by: KPMG's Creative Services. **Publication Date:** December 2021. (7148)