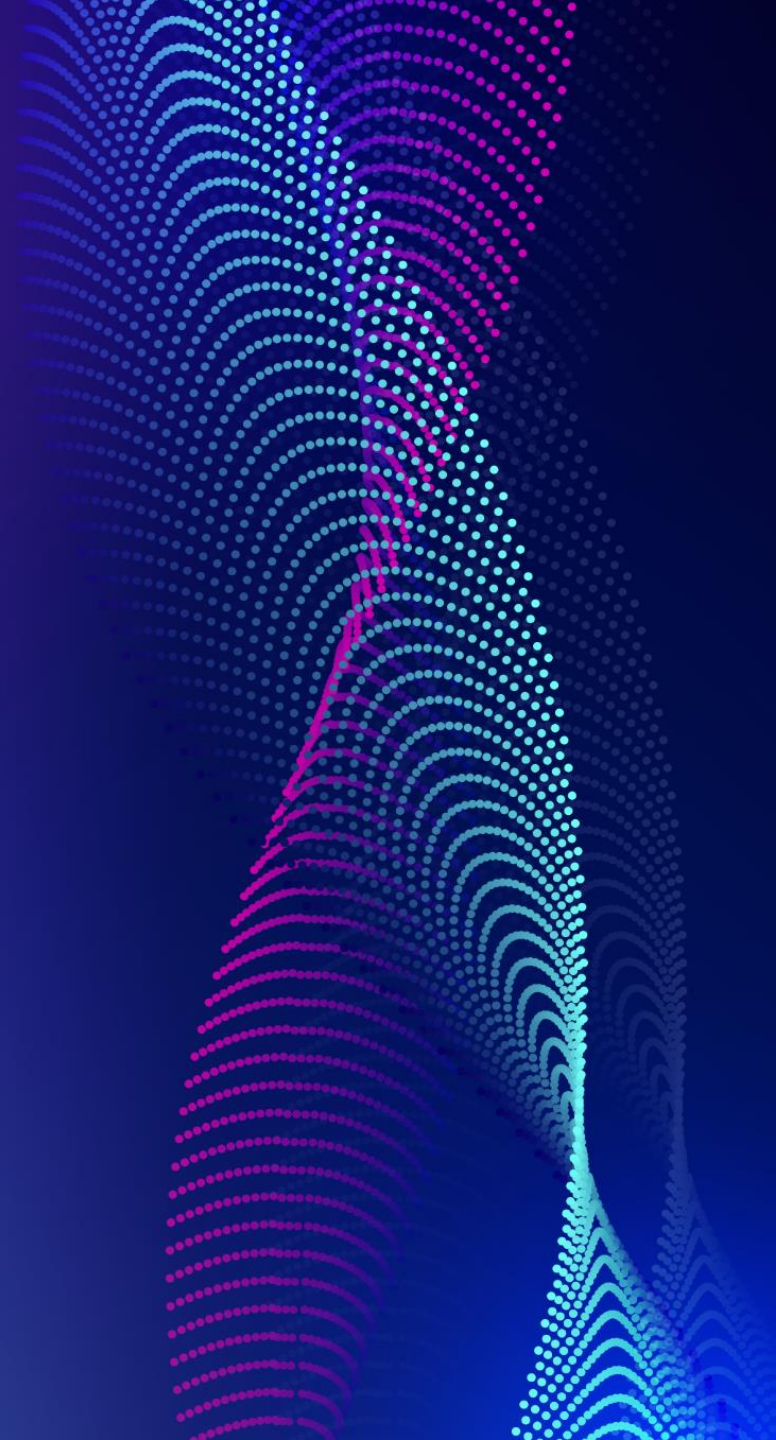
KPMG

Operational Resilience

Brian Morrissey, KPMG

July 2021



What is Operational Resilience?

Operational Resilience has been described as "The ability of firms and the financial system as a whole to absorb and adapt to shocks, rather than contribute to them". Operational resilience has rapidly moved up the regulatory agenda in the face of technology issues, supply chain and cyber concerns.

It represents a fundamental shift in how financial service firms should approach disruptive incidents and in future will mean that firms are assessed by regulators not only in terms of financial but also operational resilience.

This new focus is a response to the increasing number of high profile and high impact incidents which have struck the financial sector across the globe, from cyber-attacks to IT failures.

Firms need to adapt and develop approaches which focus on managing disruption, whatever the cause, and ensure the continuity of "critical services".

Operational Resilience is not a new concept, firms will be familiar with planning for disruption through business continuity planning and operational continuity in resolution programmes.

However regulators are concerned that the financial services industry has not adapted quickly enough to the challenges of a more connected world.

Challenges of a more connected world include:

- Increased system complexity
- Vulnerabilities due to interconnectedness
- Changing customer behaviours
- Competitive pressures and the increased risk of cyber-attack

The Global Regulatory Landscape

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 based on the UK's work. Operational Resilience is a new consideration all financial services firms will need to adapt to going forward.

The United Kingdom

- PRA: Speech on BoE approach to operational resilience and questionnaire released in June 2017
- PRA: FCA Technology & Cyber Resilience Questionnaire in Feb 2018
- PRA: Speech on Resilience and continuity in an interconnected and changing world in June 2018
- PRA / FCA/ BoE Discussion paper released in July 2018
- Consultation paper setting out draft regulatory requirements due Q3 2019

The United States of America

- Increasing focus on Cyber.
- Leading thinking on 'safe harbour'.
- Third Party Risk is key focus.
- FSSCC: Operational Resilience White Paper, March 2019

The European Union

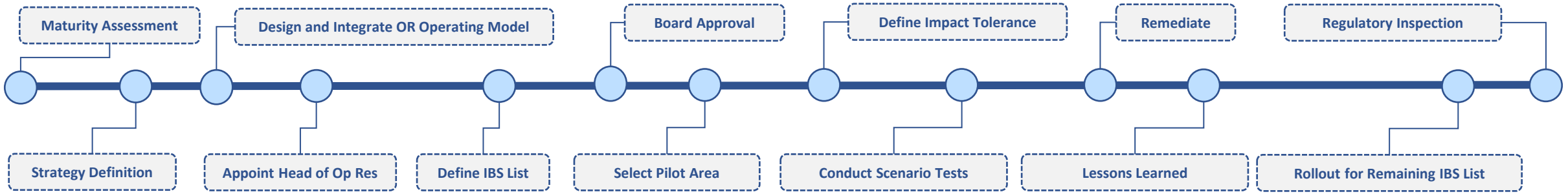
- CBI: Discussion paper on outsourcing and OCIR
- EBA: Recognising wider agenda but still issuing guidance on individual elements.
- For example, outsourcing to cloud and other arrangements.
- Also a CP on ICT and security management in December '18
- ECB: IT risks and cyber resilience are part of the 2019 SSM priorities

Related Regulatory Requests

- JST: IT Questionnaire 2019
- JST: Cyber deep dive in Dec 2018
- FCA: Multi-firm review on operational resilience Autumn 2018
- JST: Review on outsourcing and supplier management Feb 2018
- PRA: Response to 2017 Questionnaire on Operational Resilience
- JST: Review on Business Model and Profitability 2017

Regulatory Compliance is Looming

Organisations are struggling to manage the onerous workload that is associated with regulatory compliance. Leading firms in the UK have found blockers along the day from technology, people, resource and technical constraints. Taking immediate action will ensure challenges are anticipated and avoided as early as possible.



2019 / 2020	2021 / 2022+

CBI Perspective				
The CBI has been gathering information on the topical globally, learning about the subject and benchmarking against other EU counterparts (and planning based off this).	A central team now exists in the CBI which indicates that Operational Resilience is likely to become a key area of focus in the coming years.	The CBI will want to start testing resiliency along a number of lenses (i.e. not just the people pillar which was tested during COVID19).	While the SSM is not as currently mature on Op Res it is expected to come as a 'Big Bang' with supervision coming fast with tight timelines.	The CBI has released the Consultation Paper for Cross Industry Guidance on Operational Resilience in April 2021 and firms will need to be in a position to evidence actions/plans to apply the guidance within 2 years of its being issued.

CBI and Operational Resilience

There has been increased regulatory guidance on Operational Resilience released over the past number of months. The Central Bank of Ireland (CBI) released their Consultation Paper for Cross Industry Guidance on Operational Resilience in April 2021 which largely aligns to the Bank of England (PRA and FCA) policy statement and BCBS principles which were released a few weeks prior.

An operationally resilient firm is **able to 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**.

Key CBI Operational Resilience Concepts

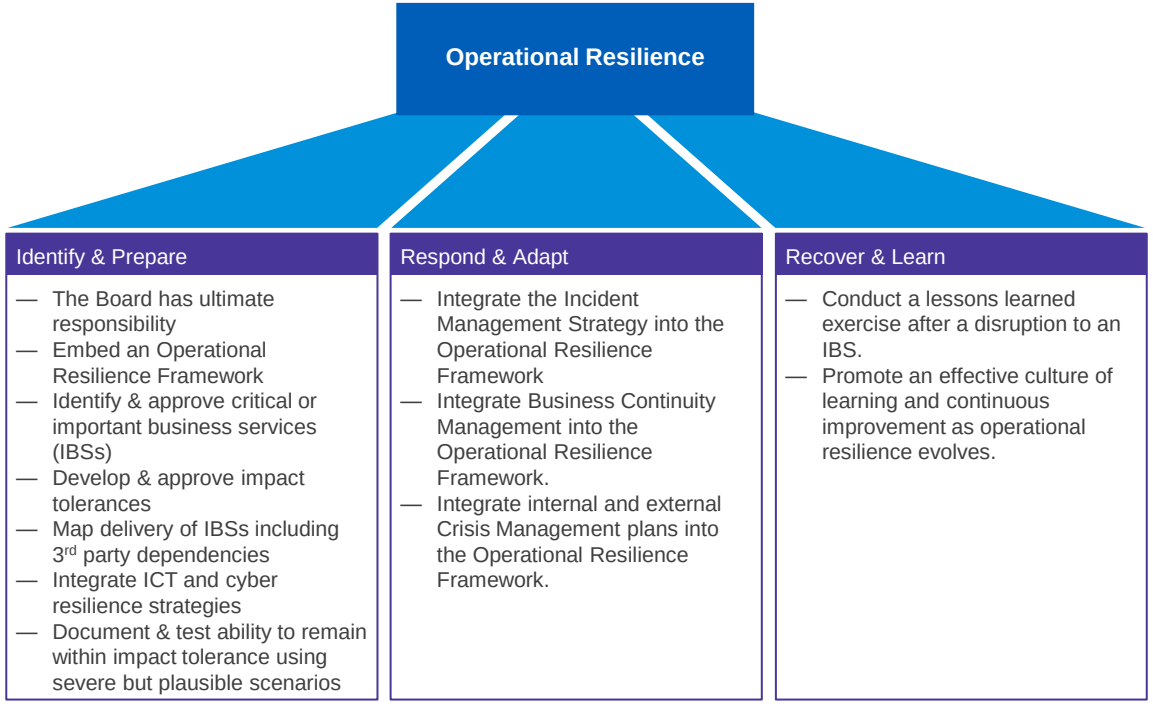
Firms should accept that disruptive events will occur and put forward-looking plans in place to deal with the events when they materialise.

Operational resilience is an evolution of operational risk and business continuity management and, as such, should be aligned with existing or developing frameworks in these areas.

A firm's operational resilience strategy should be cause agnostic and flexible enough to adapt to different types of disruption.

Operational Resilience is an opportunity to improve decision-making and value creation by targeting investment into the services that are critical or important to a firm and the economy

Central Bank Guidance is built around three pillars of Operational Resilience:

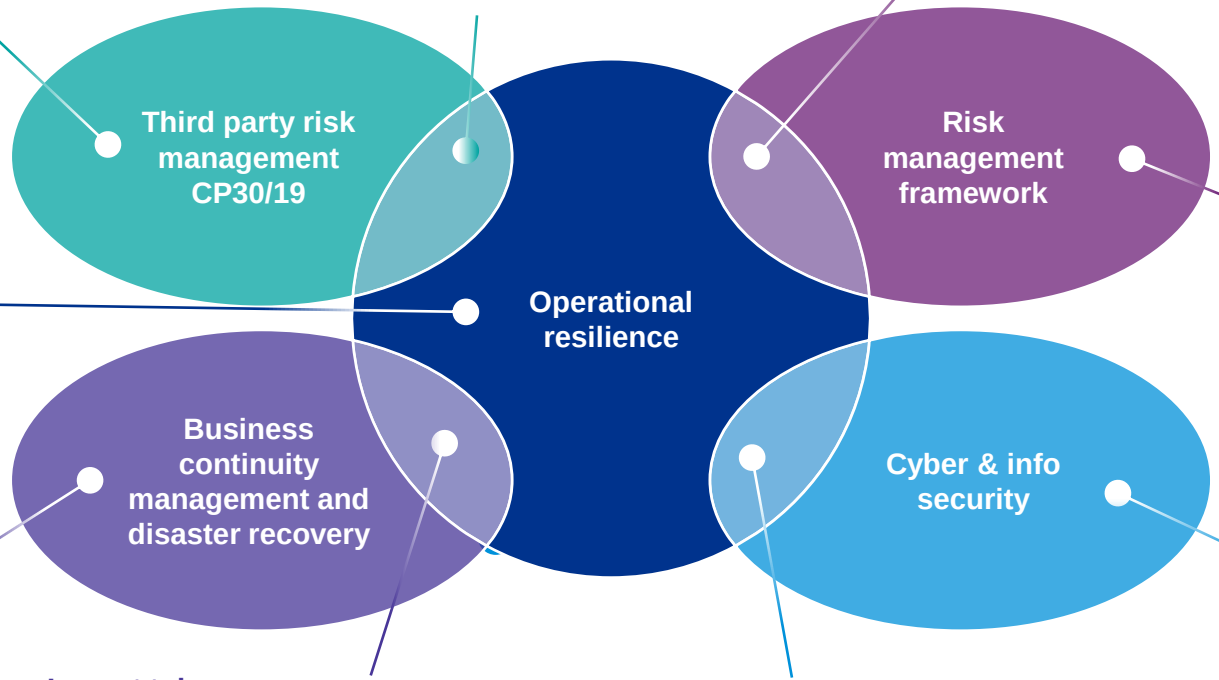


Operational Resilience – What is Different?

- Look into 3rd & 4th parties - materiality
- Governance & records
- Data and controls
- Scenarios and testing
- Exit & recovery strategies

- Contracting
- Risk assessments
- Access & audit
- Ex ante

- Severe but plausible disruption scenarios
- Risk register and risk appetites
- 1st line risk controls and metrics



New in operational resilience:

- Holistic, end to end important business services
- Customer focus
- Impact tolerances
- More Board ownership
- People pillar
- Resilience reporting
- Holistic testing

- Ex ante risk mitigation strategies
- Functional approach
- 2nd line lens/challenge
- Risk aggregation & reporting

- Asset/team-silo based
- RTO/RPO
- Max tolerable downtimes

- Impact tolerances
- Scenarios and testing
- Recovery playbooks
- Configuration management

- Governance
- Controls & metrics: identify, respond, recover
- Pen testing/vulnerability management

- Detect, protect
- Asset-based security
- Privacy/GDPR
- Data & security architecture, incl cloud
- Privileged access mgmt
- Centralised security monitoring

KPMG

kpmg.ie