WILLIAM FRY

// ASSET MANAGEMENT & INVESTMENT FUNDS

Operational Resilience Guidance Published by the Central Bank

December 2021

On 1 December 2021, the Central Bank published cross-industry operational resilience guidelines (the **Guidelines**) for regulated financial service providers (**RFSPs**). The Guidelines, which were preceded by an industry consultation process (CP140) earlier this year, set out a recommended approach for ensuring operational resilience through the management of disruptive events under the three pillars of (i) identify and prepare; (ii) respond and adapt; and (iii) recover and learn.

The Guidelines, which are additional to and do not supersede RFSP governing regime rules, should be applied by RFSPs on a propionate basis taking account of a firm's nature, scale and complexity.

Why the current focus on operational resilience?

The Guidelines highlight three main drivers of the focus on operational resilience; accelerated dependence on technology (including as a result of the COVID pandemic), increasingly complex outsourcing structures; and notwithstanding recent international policy initiatives (e.g. forthcoming European Digital Operational Resilience Act (DORA)), the absence of one clear, detailed international standard for operational resilience. The Guidelines seek to address this last point by establishing a holistic approach to operational resilience management which will allow firms operating cross-border to develop operational resilience frameworks that address regulatory concerns arising from the increased levels of dependence on technology and outsourced service providers.

How does operational resilience management interact with existing operational risk and business continuity management?

"The Central Bank considers operational resilience to be the ability of a firm.. to identify and prepare for, respond and adapt to, recover and learn from, an operational disruption. The first step in becoming operationally resilient is accepting that disruptive events will occur, and that these events need to be managed effectively."

The focus of the Guidelines is on the establishment of a board-level, forward-looking framework which will facilitate a firm's effective management of risk events when they materialise. While RFSPs are already subject to, under their respective governing regimes and related regulatory guidance, requirements for the adoption and implementation of operational risk management frameworks with the objective of preventing and mitigating against such events, the necessity for operational resilience frameworks is born from the reality that such events will and do occur and firms should therefore prepare to effectively manage the consequential disruption to their operations. However, the Central Bank considers operational resilience to be *"an evolution"* of operational risk and, as such, firms' operational resilience management frameworks should be aligned with existing operational risk management frameworks but should go beyond minimising risk and focus on capabilities to deal with risk events when they inevitably materialise.

In addition to aligning with the operational risk management framework, firms' operational resilience frameworks should also draw from and seek to support the business continuity planning of RFSPs. While the Central Bank considers operational resilience to be "*much wider than just continuity and recovery",* as it also

includes incident management and management of operational risk, third party risk, and IT and cyber risk, the continuity of critical or important business services is an essential component of being operationally resilient. Accordingly, the Central Bank recommends that operational resilience management frameworks align with and build on firms' existing business continuity plans.

When do firms need to implement the Guidelines?

The Central Bank expects firms to "*actively and promptly*" address operational resilience vulnerabilities and be in a position to evidence actions/plans to apply the Guidelines, at the latest, within two years of issuance of the Guidelines (i.e. by 1 December 2023). Evidence of actions/plans that the Central Bank will look for include:

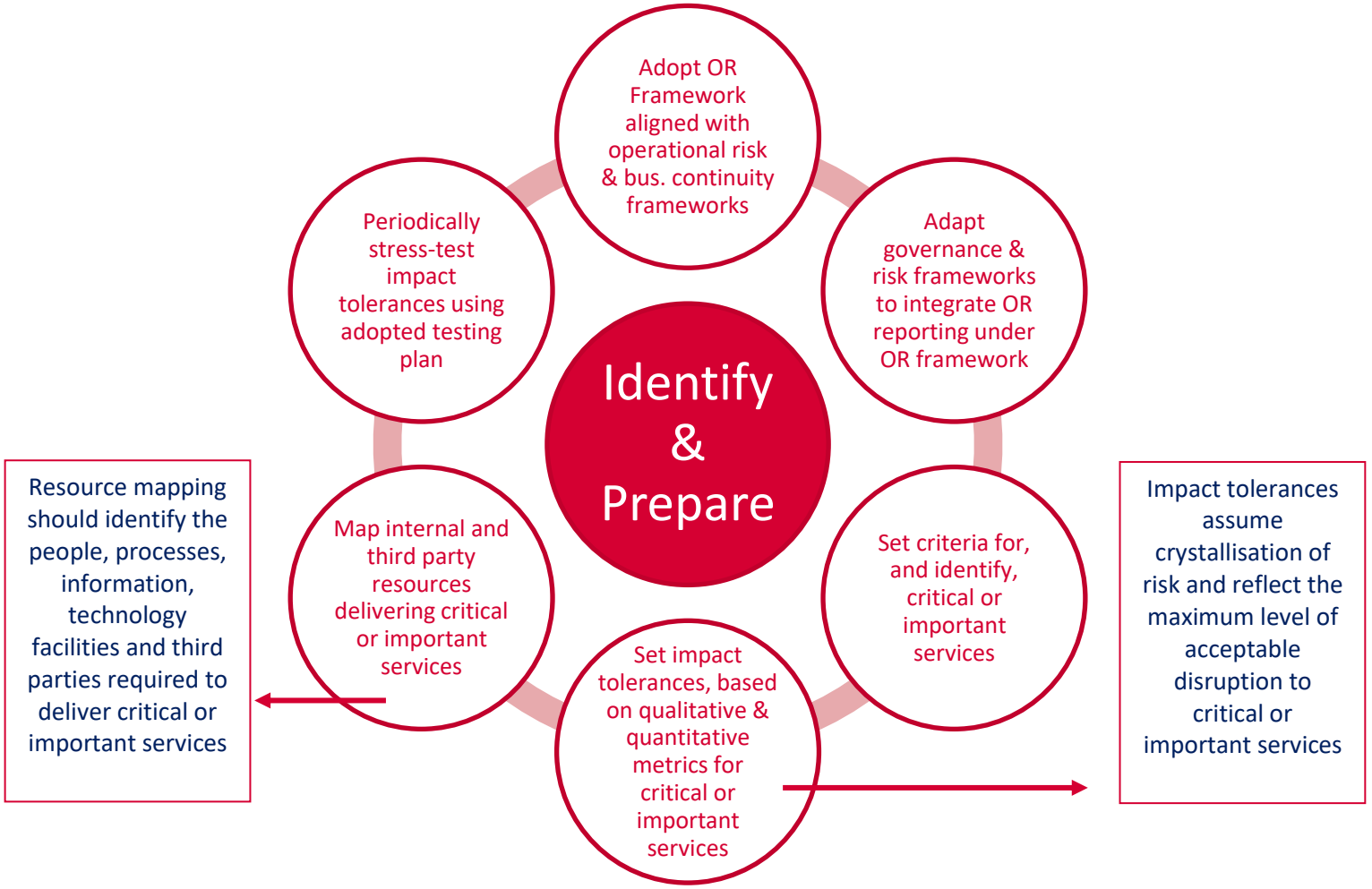
- Board ownership and accountability for an adopted operational resilience framework;
- the Board seeking the required information to enable understanding of the risk and resilience profile of the firm and making targeted investment decisions to support ongoing resilience efforts;
- the firm developing an understanding of the delivery of critical or important business services, the people, the activities, information, technology, and third parties that support that delivery, and the criticality of those services to the wider financial system;
- determination of appropriate impact tolerances for critical or important business services and that they test their ability to remain within those impact tolerances under severe but plausible scenarios; and
- consideration of third parties in the response and recovery processes and that they are aligned and tested for effectiveness.

The Guidelines

As mentioned above, the Guidelines set out a three-pillar approach to operational resilience management.

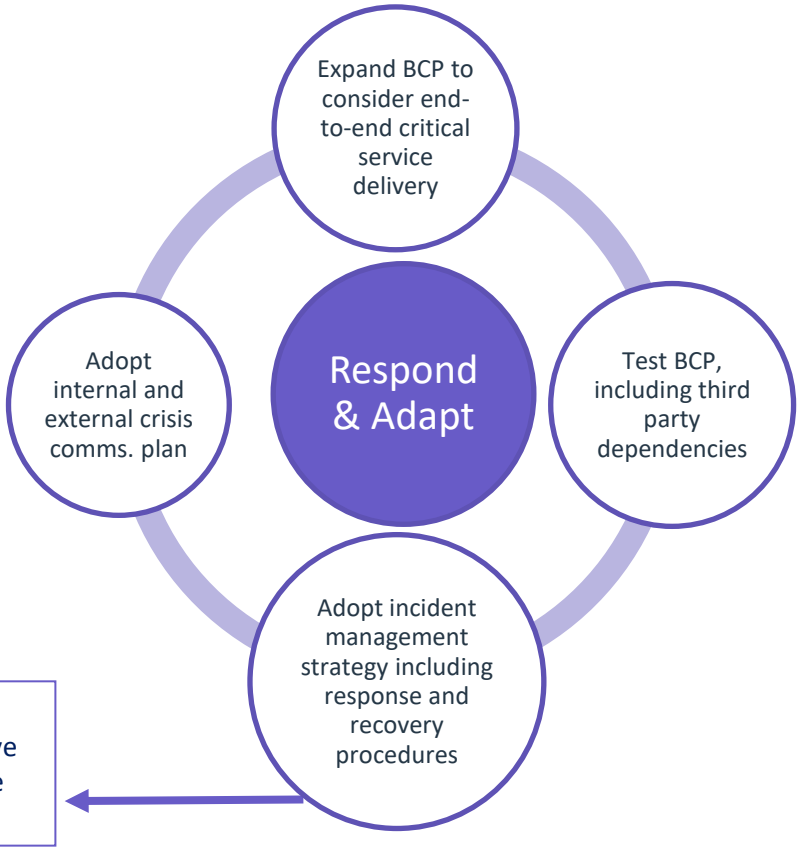
Pillar 1: Identify & Prepare

Under the first pillar of 'Identify and Prepare', there are six guidelines which, in summary, recommend the adoption and ongoing review (at least annually) by the Board of an operational resilience (**OR**) framework that provides for the classification of 'critical or important' services and the establishment of service impact tolerances setting out the firms' maximum tolerance for disruption to critical services.



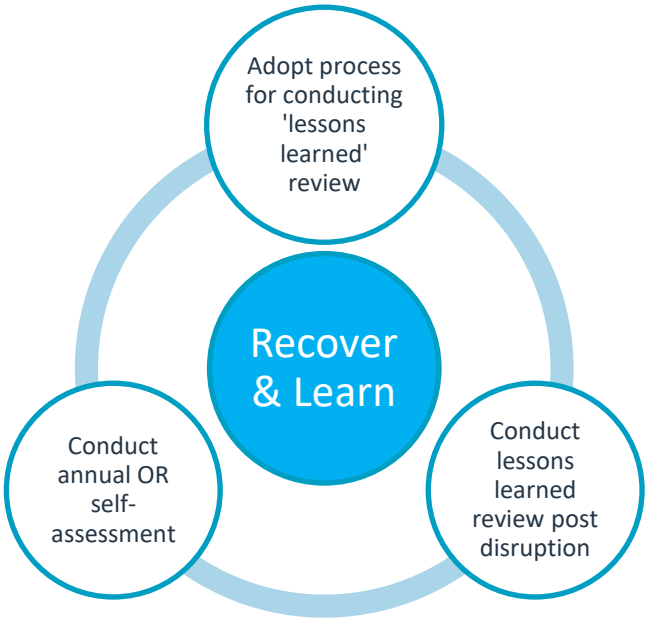
Pillar 2: Respond & Adapt

Under the second pillar of 'Respond and Adapt', there are four guidelines which, in summary, recommend that firms' OR frameworks incorporate an expansion of existing business continuity planning (**BCP**) beyond single-point failures to address continuity planning for critical services on an end-to-end delivery basis.



Incident management strategies should classify potentially disruptive incidents and identify appropriate responses

Pillar 3: Recover & Learn



Under the third pillar, the Central Bank expects firms' OR frameworks to provide for the performance of 'lessons learned' exercises after a disruption to a critical or important service including, for example:

- How and why the incident occurred;
- The identified vulnerabilities;
- The impact on the delivery of the service;
- Whether the risk controls, decisions and recovery processes and communications were appropriate; and
- The speed of recovery and whether the impact tolerances are adequate

WILLIAM FRY

DUBLIN | CORK | LONDON | NEW YORK | SAN FRANCISCO | SILICON VALLEY

William Fry LLP | T: +353 1 639 5000 | E: info@williamfry.com

williamfry.com