May 2021

CBI Consultation on Cross Industry Guidance on Operational Resilience ("CP140")

The Central Bank of Ireland (the "**CBI**") has published, CP140, which seeks views from interested stakeholders on the CBI's proposed Cross Industry Guidance on Operational Resilience (the "**Guidance**").

When developing the Guidance, the CBI has had regard to a number of matters including: (a) that there has been an increased dependence on technology, coupled with an accelerated pace of change, which has led to a rise in operational incidents across all sectors in recent years; (b) the COVID-19 pandemic has put firms' operational resilience to the test and highlighted the importance of being more operationally resilient; (c) changing customer behaviour is putting pressure on firms to enhance their digital offerings and has placed a different type of stress on how firms operate; (d) the Operational Resilience Maturity Assessment (the "**OR Assessment**") issued by the CBI to a large cohort of firms across the financial system in Q4 of 2020. The objective of the OR Assessment was to develop an understanding of the common issues faced by firms and to provide an insight into firms' resilience capabilities; and (e) the CBI's strategic commitment to "strengthening resilience" throughout the financial system, as outlined in their 2019-2021 Strategic Plan.

Purpose of the Guidance

While acknowledging that not all potential hazards can be prevented, the CBI believes that a flexible, pragmatic and proportionate approach to operational resilience will strengthen the industry's ability to respond to and recover from such events. In particular, the CBI outlines that the purpose of the Guidance is to:

- Communicate to the Boards and senior management of Regulated Financial Service Providers ("**RFSPs**") the CBI's expectations with respect to the design and management of operational resilience;

For further information on any of the issues discussed in this article please contact:

Emmet Quish
DD: + 353 (0)1 673 1724
emmet.quish@dilloneustace.ie

Hannah Fenlon
DD: + 353 (0)1 674 1005
hannah.fenlon@dilloneustace.ie

- Emphasise Board and senior management responsibilities when considering operational resilience as part of their risk management and investment decisions; and
- Require that the Boards and senior management take appropriate action to ensure that their operational resilience frameworks are well designed, are operating effectively, and are sufficiently robust.

This should ensure that the risks to the RFSP's operational continuity do not transmit into the financial markets and that the interests of the customers and market participants are safeguarded during business disruptions.

What is Operational Resilience and who will be subject to the Guidance?

Operational resilience ("**OR**") is the ability of the RFSP, and the financial services sector as a whole, to identify and prepare for, respond and adapt to, recover and learn from an operational disruption. The CBI sets down that an operationally resilient RFSP is able to recover its Critical or Important Business Services[1] from a significant unplanned disruption, while minimising impact and protecting its customers and the integrity of the financial system.

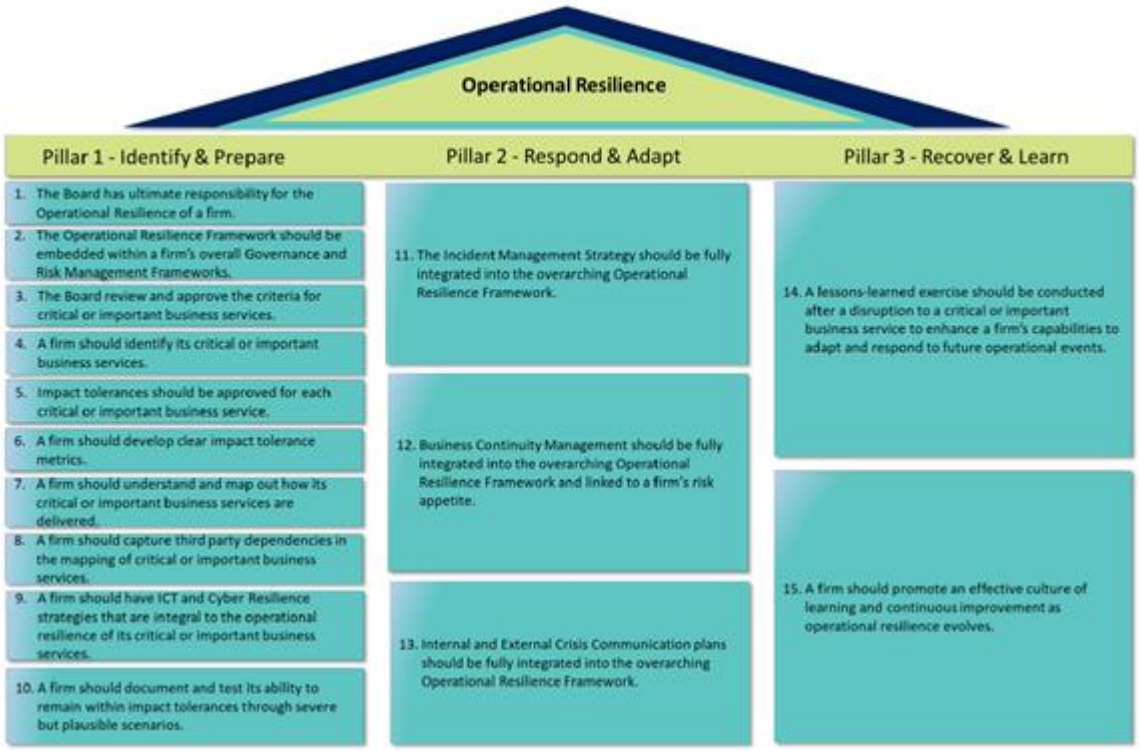
The CBI are proposing to apply the Guidance to all RFSPs, as defined in Section 2 of the Central Bank Act 1942. This means that a number of firms regulated by the CBI including, but not limited to, investment funds, fund management companies, investment managers, depositaries and administrators will be subject to the Guidance.

The Guidance

The Guidance is not prescriptive or at a granular level of detail and is designed to be flexible and can be applied by RFSPs in a proportionate manner based on the nature, scale and complexity of their business. The Guidance should be read in conjunction with the relevant legislation, regulations, and other guidance or standards issued by the European Supervisory Authorities ("**ESAs**") or the CBI. The Guidance does not supersede existing sectoral legislation, regulations, or guidance but is intended to complement and support them. The CBI may update or amend the Guidance from time to time.

The Guidance is built around three Pillars of OR with guidelines in each Pillar. The guidelines within each Pillar are grouped into various themes which we have sought to summarise below.

[1] Business Services and Critical or Important Business Service are as defined in CP140



Governance – Guidelines 1 & 2

The CBI expects a Board[2] and senior management driven focus on OR within the RFSP in order to ensure that resilience is built into the RFSP's priorities and strategic decision-making and ensuring Critical or Important Business Services are made more resilient. The CBI views management of the RFSP's operational risk and resilience as a unified objective, enacted through one consistent framework drawing from elements of business continuity, third party risk management, Information Communication Technology ("**ICT**") and cyber risk management, incident management as well as the wider aspects of operational risk management. The RFSP should develop a documented OR framework incorporating the Operational Risk and Business Continuity frameworks which will then be strategically implemented across the business by senior management throughout the Operations, Risk and Finance teams of the RFSP.

Boards should have sufficient understanding to provide effective oversight of the RFSP's OR. This means that formal OR management information should be embedded into the Board reporting structure so that OR management information is provided to the Board on a regular basis and in the event of a disruption.

The Board should review and approve all elements of the OR framework at least annually. The Board should also test the RFSP's assessment of its Critical or Important Business

[2] As defined in CP140.

Services, Impact Tolerances[3], business service maps and scenario analyses at least annually and/or as part of any review carried out after a disruption has occurred.

Identification of Critical or Important Business Services – Guidelines 3 & 4

The Board of the RFSP must approve a clearly defined and documented criteria to determine how business services are classified as critical or important. This should be achieved by considering the risk a disruption poses to customers, the RFSP's viability, safety and soundness and to overall financial stability. Once the criteria have been set, the RFSP should identify its Critical or Important Business Services and consider whether the number of Critical or Important Business Services are proportionate to its business size. The criteria should be reviewed and approved by the Board annually or at the time of implementing a material change to the business that would involve additional Critical or Important Business Services.

Impact Tolerances – Guidelines 5 & 6

The purpose of an Impact Tolerance is to quantify the maximum acceptable level of disruption to a Critical or Important Business Service. The RFSP should set at least one Impact Tolerance metric for each of its Critical or Important Business Services. The tolerance metrics need to be clear, measurable and set at the point at which the disruption to the RFSP's business service would pose, or have the potential to pose, a risk to the RFSP's viability, safety and soundness, to financial stability or could cause material detriment to customers. Impact Tolerances will be required to be tested against severe but plausible scenarios to determine their appropriateness. The Board of the RFSP should review and approve the Impact Tolerances at least annually or when a disruption occurs.

Mapping of Interconnections and Interdependencies – Guidelines 7 & 8

In order to ensure that a Critical or Important Business Service can remain within its Impact Tolerance(s) the RFSP needs to understand how the services are delivered and how each service can be disrupted. As a result, the Guidance provides that the RFSP should identify, document and map the necessary people, processes, technology, facilities, third party service providers and information required to deliver each of its Critical or Important Business Services.

Mapping[4] should be undertaken collaboratively across the business of the RFSP and should be detailed enough to enable (a) the identification of the resources that contribute to the delivery of each stage of the services, and their importance, (b) the identification of vulnerabilities and key dependencies and (c) to support testing of the RFSP's ability to stay within the assigned Impact Tolerance(s). As part of the Mapping, the RFSP should identify which business units own each resource and where it is provided from. External dependencies in respect of the delivery of key elements of the RFSP's Critical or Important Business Services should also be clearly captured and detailed in the Mapping process.

The CBI goes on to outline in the context of outsourcing, that the RFSP should ensure that third party arrangements have at least equivalent OR conditions as the RFSP and that legally binding written agreements are in place with third parties that detail how the Critical

[3] As defined in CP140
[4] As defined in CP140

or Important Business Services will be maintained during a disruption. Guideline 8 should be read in conjunction with the CBI's Cross Industry Guidance on Outsourcing. In this regard, see the Dillon Eustace briefing on the Central Bank's proposed new cross-industry guidance on outsourcing.

ICT and Cyber Resilience – Guideline 9

The Guidance highlights that RFSPs should ensure that their ICT is robust and resilient and is subject to protection, detection, response and recovery programmes in line with industry best practice. In addition, the Mapping process outlined above should include the identification of where technology is part of the delivery of a Critical or Important Business Service and the steps outlined in Guidelines 7 and 8 should be taken where IT systems or technology resources are provided by a third party.

The CBI expects that ICT systems and their cyber resilience should be regularly tested as part of severe but plausible Scenario Testing[5]. Ongoing threat intelligence and situational awareness programmes should feed into the OR programme. Guideline 9 should be read in conjunction with the CBI's "Cross Industry Guidance in respect of Technology and Cybersecurity Risks".

Scenario Testing - Guideline 10

RFSPs should test their ability to remain within their Impact Tolerance for every Critical or Important Business Service through severe but plausible scenarios. The RFSP should identify an appropriate range of adverse circumstances to its business and risk profile and consider the risks to delivery of the Critical or Important Business Services in those circumstances. The nature and frequency of testing should be proportionate to the RFSP's size and complexity but should at least be completed annually and the testing should be documented. The Board of the RFSP should review the results of the testing and if the testing identifies where Impact Tolerances may be breached then it is the responsibility of the Board and senior management to take action to improve the resilience of the business service and focus investment where needed.

Business Continuity Management – Guideline 11

The CBI expects that business continuity management ("**BCM**") needs to be fully integrated within the OR framework and in order to do this, business continuity plans should be tested through severe but plausible scenarios and include any third party interdependencies or interconnections.

As part of the Mapping outlined earlier, RFSP's should develop a disaster recovery plan in line with approved Impact Tolerances.

The CBI reiterates that key personnel should have necessary training to ensure they can execute contingency plans when responding to disruptions. Also, the arrangement with third parties for the delivery of Critical or Important Business Services should be reviewed at least annually and the RFSP should consider identifying interdependencies that can be substituted in the event of an unexpected disruption.

[5] As defined in CP140

Incident Management - Guideline 12

The CBI considers that incident management is an essential component of being operationally resilient. In this regard, incident management needs to be fully integrated within the OR framework. In order to do this, RFSPs should develop and implement response and recovery plans and procedures to manage incidents that have the potential to disrupt the delivery of Critical or Important Business Services. The incident management plans should be developed to consider how a disruption can affect the RFSP's risk appetite and Impact Tolerances.

The RFSP should maintain an inventory to support the RFSP's response and recovery capabilities that includes incident response and recovery steps followed during a disruption, internal and third party resources potentially impacted and communication plans followed. Comprehensive incident response and recovery procedures should be periodically reviewed, tested and updated.

Communication Plans – Guideline 13

The Guidance outlines that crisis communication plans (including internal and external communications) should be developed by the RFSP as part of the OR framework or in the BCM or disaster recovery plan. An effective crisis communication plan will identify the key resources and experts that can be leveraged when a disruption occurs.

Lessons Learned Exercise and Continuous Improvement – Guidelines 14 & 15

The Guidance highlights that RFSPs should conduct a "lessons learned" exercise after any disruption to a Critical or Important Business Service. This includes any potential material disruption to a third party provider that feeds into the delivery of a Critical or Important Business Service. This exercise allows the RFSP to reflect on the three-Pillar approach to OR and allows for a feedback loop into the first two Pillars which encourages improvement. The RFSP should have pre-determined criteria or questions that form the basis of the lessons learned exercise and the Guidance outlines four minimum considerations in this regard. Remedial action can then be identified and consideration should be given to whether Impact Tolerances need to be adjusted. This should all be contained within a self-assessment document and presented to the Board of the RFSP on completion.

As changes to operational approaches or technology infrastructure mature over time, there should be corresponding improvements to OR and the RFSP should promote an effective culture of learning and continuous improvement as OR evolves. RFSPs should determine the impact of strategic changes on the delivery of Critical or Important Business Services or any of the chain of activities that been documented as part of the Mapping exercise.

The RFSP should document and update written self-assessments highlighting how the RFSP meets current OR policy requirements on at least an annual basis and the review should cover all three Pillars of OR.

Submission of responses to CP140

The CBI invites feedback on the Guidance and to consider a list of specific questions outlined in CP140. The CBI requests that feedback submissions are made in writing using

the template provided in Schedule 2 of CP140, preferably as a word document or a pdf document. Respondents are requested to provide their feedback either by email to Opresilience@centralbank.ie with the subject heading in their email entitled "Consultation on Cross Industry Guidance on Operational Resilience" or, if making a submission in written correspondence, to Consultation Paper 140, GOR, Central Bank of Ireland, PO Box 559, Dublin 1. Please note that the CBI will not consider submissions which do not use the template in Schedule 2 of CP140. The closing date for submissions to the CBI on CP140 is **9 July, 2021**.

Implementation of the Guidance and Supervisory Approach

Once the Guidance is finalised, the CBI expects Boards and senior management of RFSPs to review the Guidance and adopt appropriate measures and improve their OR frameworks accordingly. RFSPs should be able to demonstrate that they have applied the Guidance within an appropriate timeframe depending on a range of factors including, inter allia, nature, scale and complexity of the RFSP's business and the RFSP's overall impact on customers and the wider economy. The CBI also expects RFSPs to be actively and promptly addressing OR vulnerabilities and be in a position to evidence actions/plans to apply the Guidance at the latest within two years of the Guidance being issued. The CBI will in the future utilise supervisory engagement to assess the core principles of OR in RFSPs.

If you have any queries in respect of the issues raised in this article or you require assistance with preparing a submission on CP140 to the CBI, please do not hesitate to contact us.

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
Tower 49, 12 East 49th Street, New York, NY10017, U.S.A. Tel: +1 646 770 6080

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.