DILLON EUSTACE

DUBLIN CAYMAN ISLANDS NEW YORK TOKYO

14 December 2021

Central Bank publishes feedback statement on Consultation Paper 140: Cross Industry Guidance on Operational Resilience

The Central Bank of Ireland (the "**CBI**") recently published its Cross Industry Guidance on Operational Resilience (the "**Guidance**") as part of its feedback statement on Consultation Paper 140 ("**CP140**"). The purpose of the Guidance is to:

- communicate to the boards (the "**Boards**") and senior management of Regulated Financial Service Providers[1] ("**RFSPs**"), the CBI's expectations with respect to the design and management of operational resilience ("**OR**");

- emphasise Board and senior management responsibilities when considering OR as part of their risk management and investment decisions; and

- require that Boards and senior management take appropriate action to ensure that their OR frameworks are well designed, operating effectively and 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.

The Guidance 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 CBI expects Boards and senior management of RFSPs to review the Guidance and adopt appropriate measures to strengthen and improve their governance and risk frameworks and their effective management of OR. A RFSP should be able to demonstrate that it has considered the supervisory expectations set out in this Guidance and developed a plan to meet the Guidance.

Key Points to Note:

- **The Guidance remains largely the same as the draft previously published in CP140.**
- **OR should be appropriately robust and effective but RFSPs can apply proportionate approach.**
- **Board and senior management have an important role to play in terms of the OR Framework.**
- **RFSPs must set criteria for defining its critical or important business services.**
- **RFSPs must be in a position to evidence actions/plans to apply the Guidance at the latest within two years of its being issued.**

Operational Resilience

OR is the ability of a 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. RFSPs will need to put in place a flexible and forward-looking OR strategy to deal with a potential range of disruptions and which

[1] The Guidance applies to all regulated financial service providers, as defined in Section 2 of the Central Bank Act 1942

ensure coordination between risk management, business continuity management ("**BCM**"), incident management, third party risk management, Information Communication Technology ("**ICT**") and cyber risk, and recovery and resolution planning.

The Guidance – Core Principles and 3 pillars of OR

The core principles of any OR Framework are:

- Board and senior management ownership of the OR Framework;

- The identification of critical or important business services and all activities, people, processes, information, technologies and third parties involved in the delivery of these services;

- The setting of impact tolerances for each of these identified services, and the testing of the RFSP's ability to stay within those impact tolerances during a severe but plausible operational disruption scenario; and

- The continuous review of how a RFSP responded and adapted to disruptive or potentially disruptive events so that lessons learned can be incorporated into operational improvements to continually enhance the OR of the RFSP.

The Guidance is built around three pillars of OR with individual guidelines which are detailed below and summarised in this briefing. The three pillars create a feedback loop that fosters the perpetual embedding of lessons learned into a RFSP's preparation for operational disruptions.

Pillar 1 Identify & Prepare – Governance

Guidance at a glance

- The Board has ultimate responsibility for the OR of a RFSP.
- The OR Framework should be aligned with the RFSP's overall Governance and Risk Management Frameworks.

The Guidance outlines that the Board of the RFSP has ultimate responsibility for the OR of a RFSP. All Board members should have sufficient understanding to provide effective oversight and challenge of the RFSP's OR.

Senior management should be given the financial, technical and other resources needed in order to support the RFSP's overall OR efforts under the oversight of the Board. The Board and senior management should have accurate and adequate oversight of resilience activity, trends and remediation measures, which allows them to make the business decisions regarding investments and risk exposure. A RFSP should provide for an appropriate periodic reporting structure with escalation routes established for when vulnerabilities are identified or when an unexpected disruption occurs.

The Board has responsibility for the approval and oversight of the OR Framework and approval of the critical or important business services, impact tolerances, business service maps, scenario testing to ascertain the RFSP's ability to remain within impact tolerances, and communications plans. The Board should review the OR Framework as least annually to confirm that there are no undetected developing weaknesses.

The Guidance sets out that a RFSP will need to ensure that its existing governance frameworks and committee structures include responsibilities with respect to OR. A RFSP should develop a documented OR Framework aligned with its Operational Risk and Business Continuity Frameworks, or include these risk areas in one holistic framework.

OR should be strategically implemented across the business by senior management throughout the Operations, Risk and Finance functions of the RFSP.

Pillar 1 Identify & Prepare – Identification of Critical or Important Business Service

Guidance at a glance

- The Board reviews and approves the criteria for critical or important business services.
- The RFSP should identify its critical or important business services.

As referenced above, the Guidance outlines that in order to begin enhancing a RFSP's OR, the RFSP should set the criteria for defining its critical or important business services. This allows the RFSP to prioritise services in the event of a disruption. As a result, the RFSP should consider the risk a disruption poses to customers, to the RFSP's viability, safety and soundness, and to overall financial stability.

It is the responsibility of the Board to approve clearly defined and documented criteria to determine how business services are classified as critical or important. This criteria should be reviewed and approved by the Board annually or at the time of implementing material changes to the business that would involve additional critical or important business services.

Once the criteria is set, the RFSP should identify its critical or important business services by looking at the complete end-to-end set of activities required to deliver a particular business service and taking an outcomes based approach to identification of these critical or important services. The RFSP should also consider whether the number of critical or important business services is proportionate to the nature, scale and complexity of its business.

It will be the responsibility of the Board to review and approve all business services classified as 'critical' or 'important' on at least an annual basis.

Pillar 1 Identify & Prepare – Impact Tolerances

Guidance at a glance

- Impact tolerances should be approved for each critical or important business service.
- A RFSP should develop clear impact tolerance metrics.

The Guidance requires that a RFSP should, following on from the above, develop impact tolerances for each of its critical or important business services on the assumption that disruptive events will happen. The purpose of an impact tolerance is to determine the maximum acceptable level of disruption to a critical or important business service and should be a standard that the RFSP remains within.

Impact tolerances should be set at the point at which 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 should be used as a planning tool for a RFSP and need to be tested against severe but plausible scenarios to determine their appropriateness.

A Board should review and approve impact tolerances at least annually or when a disruption occurs to determine if the original approved impact tolerances are still fit for purpose.

There should be at least one impact tolerance metric for each of a RFSP's critical or important business services. Impact tolerance metrics need to be clear and measurable, and can be both qualitative and quantitative.

Pillar 1 Identify & Prepare – Mapping of Interconnections and Interdependencies

Guidance at a glance

- The RFSP should understand and map out how its critical or important business services are delivered.
- A RFSP should capture third party dependencies in the mapping of critical or important business services.

Once the impact tolerances are identified, a RFSP should identify, document and map the necessary people, processes, information, technology, facilities, and third party service providers required to deliver each of its critical or important business services. This exercise should be undertaken collaboratively across the business to ensure comprehensive mapping.

The mapping should of sufficient detail that (a) enables the identification of the resources that contribute to the delivery of each stage of the service, and their importance and (b) allows the RFSP to identify vulnerabilities and key dependencies, and to support testing of its ability to stay within the assigned impact tolerances for each critical or important business service.

As part of the mapping, a RFSP should identify which business units own each resource and from where it is provided. A RFSP's critical or important business services should be able to remain within impact tolerances, including when they rely on Outsourced Service Provider ("**OSPs**"). A RFSP should undertake due diligence in respect of its OSPs prior to entering into an outsourcing arrangement, to ensure that third party arrangements have appropriate OR conditions that enable the RFSP to remain within its impact tolerances.

A RFSP should ensure that legally binding written agreements are in place with third parties that detail how the critical or important services will be maintained during a disruption and an exit strategy if/when the service cannot be maintained. A RFSP should also take into account the geographical location of the third party, which may impact on the provision of the service depending on the nature or location of the event.

A RFSP should also be aware of any chain outsourcing that exists and should manage and monitor accordingly.[2]

Pillar 1 Identify & Prepare – ICT and Cyber Resilience

Guidance at a glance

- A RFSP should have ICT and Cyber Resilience strategies that are integral to the OR of its critical or important business services.

A RFSP should ensure that its information and communication technology is robust and resilient and is subject to protection, detection, response and recovery programmes in line with industry best practice. As part of the mapping process, a RFSP should identify where technology is part of the delivery of a critical or important business service and where IT systems or technology resources are provided by a third party.

The identified systems should be regularly tested as part of IT security, cyber-security and resilience testing, using severe but plausible scenarios, to ensure continuity of critical or important business services during severe disruptions.

On-going threat intelligence and situational awareness programmes should feed into the OR programme and align with the RFSP's IT risk management, IT security management, IT incident management and IT continuity/disaster recovery programmes.[3]

Pillar 1 Identify & Prepare – Scenario Testing

Guidance at a glance

- A RFSP should document and test its ability to remain within impact tolerances through severe but plausible scenarios.

Once clear and detailed maps have been developed for critical or important business services, then the RFSP should test its ability to remain within its impact tolerances, for every critical or important business service, through severe but plausible scenarios.

The nature and frequency of testing should be proportionate to the RFSP's size and complexity. This should at least be completed annually for all RFSPs. However, a RFSP that implements change more regularly should undertake more frequent testing.

[2] This aspect of the Guidance should be read in conjunction with the Central Bank's "Cross Industry Guidance on Outsourcing " and the forthcoming DORA in relation to ICT OSPs.

[3] This aspect of the Guidance should be read in conjunction with the Central Bank's "Cross Industry Guidance in respect of Technology and Cybersecurity Risks ", any relevant European Supervisory Authority Guidance, including the EBA Guidelines for ICT and Security Risk Management , the EIOPA Guidelines for ICT Security and Governance , and the forthcoming DORA and NIS2.

The Board should review the results of all scenario testing carried out on critical or important business services. If scenario testing identifies a situation where impact tolerances may be breached then it would be the responsibility of the Board and senior management to take action to improve the resilience of the business service and focus investment where needed. The design and implementation of remediation plans are the responsibility of senior management and the results of the remediation plans should be reviewed and approved by the Board thereafter.

Pillar 2 Respond and Adapt – Business Continuity

Guidance at a glance

- BCM should be fully integrated into the overarching OR Framework and linked to a RFSP's risk appetite.

While OR is much broader than traditional BCM and recovery, approved business continuity plans ("**BCP**") should be utilised as part of the holistic response to a disruption.

When a disruption occurs to a RFSP's critical or important business services, the BCP should be enacted as part of the response process. For BCM to be aligned with the OR Framework, the BCP should be tested through severe but plausible scenarios and include any third party interdependencies or interconnections. To respond effectively to a disruption, an integrated BCP should incorporate invocation processes, impact analyses, recovery strategies, training programmes and crisis management programmes to guide the management of a disruption and limit the impact.

As a result, a RFSP should adopt a holistic approach to BCM by mapping critical or important business services, as outlined above, and develop a recovery plan in line with approved impact tolerances.

The Guidance outlines that key personnel should be identified and have completed the necessary training which should be customised based on specific roles to ensure that staff can effectively execute contingency plans when responding to a disruption.

Where interdependencies on third parties for the delivery of critical or important business services have been identified, it should be verified that these arrangements have appropriate OR conditions to ensure the RFSP can remain within its impact tolerances. The arrangements should be reviewed and tested at least annually and the RFSP should consider identifying the dependencies that can be substituted in the event of an unexpected disruption.

Pillar 2 – Incident Management

Guidance at a glance

- The Incident Management Strategy should be fully integrated into the overarching OR Framework.

The RFSP's incident management strategy should be fully integrated into the overarching OR Framework. As a result, the RFSP 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. When responding to an incident, the incident management plans should be developed to consider how a disruption can affect a RFSP's risk appetite and impact tolerance metrics.

A RFSP should maintain an inventory to support the RFSP's response and recovery capabilities that includes the incident response and recovery steps followed during a disruption, internal and third party resources potentially impacted, and communication plans followed.

Incident response and recovery procedures should be reviewed, tested and updated at least annually.

Pillar 2 – Communication Plans

Guidance at a glance

- Internal and External Crisis Communication plans should be fully integrated into the overarching OR Framework.

A crisis communication plan should be developed either as part of a RFSP's OR Framework or contained in the BCM/recovery plans to communicate effectively during a disruption.

The RFSP should develop internal and external communication plans and stakeholder maps that can be implemented during a disruption. The internal communication plan should contain escalation routes on how to communicate with key-decision makers, operational staff and third parties if necessary. The external communication plan should outline how the RFSP will communicate with their customers, stakeholders and regulators during a disruption.

Pillar 3 Recover and Learn - Lessons Learned Exercise and Continuous Improvement

Guidance at a glance

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

A lessons learned exercise should be conducted 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.

A RFSP should have predetermined criteria or questions that form the basis of the lessons learned exercise. These questions should identify deficiencies that caused a failure in the continuity of service and, these deficiencies should be addressed as a matter of priority.

The lessons learned exercises should define effective remediation measures to redress deficiencies and failure in the continuity of service which should be contained within a self-assessment document and presented to the Board.

OR needs to be a fundamental element of any strategic decision taken by a RFSP. A RFSP should determine the impact of strategic changes on the delivery of critical or important business services or any of the chain of activities that have been documented as part of the mapping exercise.

Furthermore, a RFSP should document and update written self-assessments highlighting how the RFSP meets current OR policy requirements on at least an annual basis. These reviews should cover all aspects of the three pillars of OR, from the identification of critical or important business services through to lessons learned exercises and ensure that no emerging vulnerabilities are overlooked.

Implementation and CBI Supervisory Approach

The CBI reminds RFSPs that OR is an evolution of operational risk and business continuity management and, as such, should be aligned with existing or developing frameworks in these areas.

The Guidance does not purport to address, in detail, every aspect of a RFSP’s legal and regulatory obligations relating to OR and should be read in conjunction with the relevant legislation, regulations, and other guidance or standards issued by the relevant industry bodies, supervisory authorities 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, in light of future regulatory requirements

RFSPs should be able to demonstrate that they have applied the Guidelines within an appropriate timeframe which will depend on a range of factors including nature, scale and complexity of a RFSP’s business and the RFSP’s overall impact on customers and the wider economy. The CBI 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 its being issued.**

The CBI has indicated that it will utilise risk-based supervisory engagement to assess the core principles of OR in RFSPs and drive to enhance and mature OR across the financial system.

If you have any questions in relation this briefing, please contact any of the authors or your usual contact in Dillon Eustace.

Dillon Eustace LLP
December 2021

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

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

DILLON EUSTACE

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

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

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

DISCLAIMER

This document is for information purposes only and does not purport to represent legal advice. If you have any queries or would like further information relating to any of the above matters, please refer to the contacts above or your usual contact in Dillon Eustace LLP.