simmons
+simmons

Central Bank of Ireland proposed operational resilience guidelines

MAY 2021

The Central Bank has launched a consultation on proposed guidelines on operational resilience. This follows the consultation on outsourcing.

Background

Operational resilience refers to the ability of a firm, and the financial services sector as a whole, to:

- identify and prepare for;
- respond and adapt to; and
- recover and learn from, an operational disruption.

Operational resilience is seen as an increasingly important area by regulators globally. Although firms are already undertaking risk management activities in specific areas such as cyber security and outsourcing, the prevailing wider view of operational resilience takes an end-to-end view of the continuity of all of a firm’s key business services.

The practical importance of operational resilience is that it improves a firm’s ability 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.

Operational risk management	The development of controls that reduce the impact and probability of an operational event occurring
Operational resilience	The development of capabilities to deal with risk events when they materialise

Proposed Guidelines

In this regard, the Central Bank of Ireland (the “Central Bank”) has launched a consultation on its proposed Cross Industry Guidance on Operational Resilience (the “Proposed Guidance”). The Proposed Guidance will apply to all regulated financial service providers (“RFSPs”) operating in Ireland. We have set out below a table showing the structure and main points of the Proposed Guidance (which is similar to the arrangements introduced by the UK financial regulators in March this year).

Pillar	Guideline	Summary
One: Identify and Prepare	**1.** The Board has ultimate responsibility for the Operational Resilience of a firm.	The board of an RFSP: • has the ultimate responsibility for approval and oversight of the **Operational Resilience Framework**; • should be provided with MI on a regular basis and in the event of disruption; and • should test the RFSP's assessment of its: ➢ critical or important business services; ➢ impact tolerances; ➢ business service maps; and ➢ scenario analyses, at least annually.
	2. The Operational Resilience Framework should be embedded within a firm's overall Governance and Risk Management Frameworks.	An RFSP should utilise its existing governance and risk management structures when implementing operational resilience and should: • develop a documented **Operational Resilience Framework** incorporating the Operational Risk and Business Continuity Frameworks; • implement operational resilience across the business throughout the Operations, Risk and Finance pillars.
	3. The Board should review and approve the criteria for critical or important business services.	Setting the criteria for defining its critical or important business services enables a firm to identify those services and prioritise them in the event of a disruption. We note also that criticality and importance is an important element of the Central Bank's proposed guidelines on outsourcing.
	4. A firm should identify its critical or important business services.	As noted above, setting the criteria for critical or important services allows their identification. The Proposed Guidance envisages a shift towards considering the complete end-to-end set of activities required to deliver a particular business service.

Pillar	Guideline	Summary	
One: Identify and Prepare	**5**. Impact tolerances should be approved for each critical or important business service.	Having identified its critical or important business services, RFSPs should develop impact tolerances for each of them, on the assumption that disruptive events will happen. In this regard, it is important to distinguish between: • risk appetite, which focuses on the impact and probability of a risk event occurring; and • impact tolerances, which assume that the risk event has already crystallised and, therefore, the probability element of risk appetite is removed. An impact tolerance quantifies the maximum acceptable level of disruption to a critical or important business service, and should be set at the point at which disruption to the firm's business service would pose, or have the potential to pose, a risk to the firm's viability, safety and soundness, to financial stability or could cause material detriment to customers.	
	6. A firm should develop clear impact tolerance metrics	RFSPs should set at least one impact tolerance metric for each critical or important business service:	
		Minimum: time-based metric	• maximum acceptable duration a critical or important business service can withstand a disruption.
		Additional metrics	• maximum tolerable number of customers effected by a disruption; • maximum number of transactions affected by a disruption; or • maximum value of transactions impacted.

Pillar	Guideline	Summary
One: Identify and Prepare	**7.** A firm should understand and map out how its critical or important business services are delivered.	Having set the impact tolerances for its critical or important business services, an RFSP now needs to ensure that they can remain within them. In order to do so, a firm should: • understand how the services are delivered and how each can be disrupted; • understand the chain of activities that contribute to the delivery of each service, to identify dependencies or vulnerabilities; • identify, document and map the necessary people, processes, technology, facilities, third parties service providers and information required to deliver each of the services.
	8. A firm should capture third party dependencies in the mapping of critical or important business services.	As noted above, the increased use of outsourcing in the financial services industry is the subject of a concurrent Central Bank consultation. It is also relevant to operational resilience because if a disruptive event occurs within an RFSP's network of outsourcing service providers ("OSPs"), the RFSP itself can be impacted. As in the draft outsourcing guidelines, the Central Bank stresses the need for RFSPs to retain visibility over their OSPs and emphasises the particular risks posed by chain outsourcing.
	9. A firm should have ICT and Cyber Resilience strategies that are integral to the operational resilience of its critical or important business services.	Again in common with the draft outsourcing guidelines, the Central Bank recognises that technology and information are key drivers and enablers of most RFSP's business models and that they should be integral to any operational resilience framework. IT systems, including the cybersecurity of these systems, should be regularly tested as part of regular testing and as part of severe but plausible scenario testing. The Central Bank also refers to its Cross Industry Guidance in respect of Technology and Cybersecurity Risks.

Pillar	Guideline	Summary
	10. A firm should document and test its ability to remain within impact tolerances through severe but plausible scenarios.	When an RFSP has mapped its critical or important business services and set its impact tolerances, it needs to test its ability to remain within those tolerances through severe but plausible scenarios. The purpose of scenario testing is to identify any vulnerabilities or reliance on third parties, and the results should focus investment in the resolvability of a vulnerable element, determine alternative channels of delivery or identify the elements that can be substituted if disrupted. The results of the testing, and any remediation plans, should be approved by the RFSP's board.
Two: Respond and Adapt	**11.** Business Continuity Management should be fully integrated into the overarching Operational Resilience Framework and linked to a firm's risk appetite.	Operational resilience is broader than BCM, because where BCM focuses on single points of failure, operational resilience goes further by determining how those points of failure have the potential to affect the end-to-end delivery of critical or important business services. The two are interconnected, because the Business Continuity Plan (BCP) will be enacted as part of the response process to a disruption of a business service. The BCP should therefore also be tested through severe but plausible scenarios.
	12. The Incident Management Strategy should be fully integrated into the overarching Operational Resilience Framework.	Incident management is another essential component operational resilience, and should therefore be fully integrated into the Operational Resilience Framework. An 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; • maintain an **inventory** to support the firm'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.

Pillar	Guideline	Summary
	13. Internal and External Crisis Communication plans should be fully integrated into the overarching Operational Resilience Framework.	An RFSP should develop **a crisis communication plan**, either as part of the Operational Resilience Framework or the BCM/Disaster Recovery (DR) plans. 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 firm will communicate with their customers, stakeholders and regulators during a disruption.
Three: Recover and 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.	A RFSP should conduct a lessons learned exercise after any disruption to a critical or important business service (including one emanating from an OSP). At a minimum, the exercise should consider: • How and why the incident occurred; • The impact on the delivery of critical or important business services; • Whether the risk controls, decisions and recovery processes and communications were appropriate; and • The speed of recovery and whether the impact tolerances are adequate.
	15. A firm should promote an effective culture of learning and continuous improvement as operational resilience evolves.	The final guideline looks at how an RFSP can make continuous improvements to its operational resilience. In order to do so, a firm must learn from its experiences as changes to its operational approaches or technology infrastructure mature over time, not only after a disruption but also as part of ongoing discussions. In addition, the final guideline states that operational resilience needs to be a fundamental element of any strategic decision taken by a firm. From a practical perspective, a firm should document and update written self-assessments highlighting how the it meets current operational resilience policy requirements on at least an annual basis.

Conclusion

In common with the recently published draft guidelines on outsourcing, our view is that the Proposed Guidelines give an insight into the Central Bank's expectations around operational resilience, and that it would be prudent for firms to use the Proposed Guidelines to carry out a gap analysis of their policies and procedures in the near term.
The Proposed Guidance should also be considered in light of the EU Commission's Digital Operational Resilience Act ("DORA") proposal which was published on 24 September 2020.

Finally, it is important for firms to remember that the Proposed Guidelines will not supersede any relevant sectoral legislation.

simmons-simmons.com.

Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word “partner” refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.