Operational resilience: Some common pitfalls in developing and implementing an effective framework

Adél Drew, FIA
Eamonn Phelan, FSAI, CERA

Milliman

In this briefing note we look at emerging experience both in the UK and Ireland in relation to the development and implementation of operational resilience frameworks, identifying some of the more common pitfalls.

The publication by the Central Bank of Ireland (CBI) of its "Cross Industry Guidance on Operational Resilience" in December 2021[1] prompted the insurance industry in Ireland to formally consider its operational resilience. Almost two years on, as the implementation deadline of December 2023 looms (by which time firms are expected to "be in a position to evidence actions/plans to apply the Guidance"), we take a look at some of the practical challenges firms have faced along the way, and which some are still working to overcome.

The CBI guidelines are well-aligned with the latest international thinking in relation to operational resilience, with the CBI citing the Basel Committee on Banking Supervision and the UK's Prudential Regulatory Authority (PRA), Financial Conduct Authority (FCA) and Bank of England amongst the bodies whose requirements and guidance have contributed to its own guidelines in this area.

In 2021, both the PRA and FCA published their operational resilience rules and guidance in PS6/21, "Operational resilience: Impact tolerances for important business services,"[2] and PS21/3, "Building operational resilience,"[3] respectively. At the same time the PRA also published SS2/21, "Outsourcing and third-party risk management to complement the requirements under operational resilience guidelines."[4] The rules and guidance came into force in March 2022 and by now all applicable firms are expected to have identified and mapped their important business services, set impact tolerances and started their programme of scenario testing. By March 2025 firms will be expected to demonstrate their ability to remain within the impact tolerances defined under a range of severe but plausible scenarios.

There are certainly many parallels between the CBI's guidance and the requirements of both the PRA and FCA, meaning that Irish firms can gain some useful insights into the challenges associated with the development and implementation of an operational resilience framework through observing experience to date in the UK. We also take a closer look at that experience here.

Recap of the CBI guidelines

Firstly, though, a quick recap of the CBI guidance. The CBI defines operational resilience as "the ability of a firm, and the financial services sector as a whole, to identify and prepare for, respond and adapt to, recover and learn from an operational disruption."

To assist firms on their journey towards operational resilience, the CBI has grouped its guidelines under three main headings, the so-called "Three Pillars of Operational Resilience," as follows:

[1] CBI (December 2021). Cross-Industry Guidance on Operational Resilience. Retrieved 23 October 2023 from https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf.
[2] Bank of England (3 June 2021). PS6/21 | CP29/19 | DP1/18: Operational Resilience: Impact Tolerances for Important Business Services. Retrieved 23 October 2023 from https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
[3] FCA (31 March 2022). PS21/3: Building Operational Resilience. Retrieved 23 October 2023 from https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience.
[4] Bank of England (29 March 2021). SS2/21 Outsourcing and Third-Party Risk Management. Retrieved 23 October 2023 from https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss.

- Identify & Prepare
- Respond & Adapt
- Recover & Learn

The first of these, Identify & Prepare, comprises 10 guidelines. These guidelines set out where responsibility lies for operational resilience within a firm; the identification of a firm's critical or important business services and impact tolerances; and understanding how these services are delivered and the extent to which they depend on third parties. They consider the role of technology and cyber resilience strategies, and the use of scenario testing to assess a firm's ability to remain within its stated impact tolerances when adverse events occur. They also address the retrofit of operational resilience requirements into the firm's existing governance and risk management frameworks, in order to achieve a unified approach to operational risk and resilience.

The second pillar, Respond & Adapt, comprises a further three guidelines. These guidelines consider the integration of business continuity management, the firm's incident management strategy and both internal and external crisis communication plans within the overarching operational resilience framework. All of these factors are components of the overall fabric of an operationally resilient firm that must be brought together to help deliver the desired outcome; however, they acknowledge that resilience goes further than crisis management, as they require delivering despite disruption and not waiting for things to "return to normal."

The third pillar, Recover & Learn, comprises the final two guidelines and is mainly concerned with continuous improvement and how it can be achieved. Operational resilience needs to include an active and effective feedback loop to help embed the learnings from the occurrence of, and response to, successive disruptive events and to foster a culture which nurtures self-assessment and self-improvement so as to continue to enhance the firm's resilience.

Experience to date

While the UK financial services regulators have not yet provided a great deal of industry feedback, they have provided some useful insights. In a speech delivered in April 2022, David Bailey, executive director for International Banks Supervision of the Bank of England, provided an initial assessment of progress by UK banks and building societies. Comments relevant to the insurance industry are discussed below.[5]

Important business services

With regard to important business services, Mr Bailey commented that for those firms which had been reviewed a wide range of levels of granularity in approach has already emerged. For example, the broad category of "payments" was identified by some organisations as an important business service, while others went down to individual systems, such as BACS etc. While it was noted that the guidance was designed to deliberately enable firms to have flexibility on the granularity defined for their unique situations, he made it clear that firms will be expected to justify how they have defined their important business services (referred to in the CBI guidance as "Critical or Important Business Services"), considering the following points:

1. The service should deliver a specific outcome or service to an identifiable external user—therefore if a firm has identified more than one outcome, or a user cannot be identified, then the granularity may be insufficient.
2. On the opposite end of the scale, the level of granularity should distinguish an important business service from an activity that represents a collection of services or an internal service—in this case the granularity may be excessive.
3. The level of granularity should facilitate the setting of one impact tolerance per regulatory objective and be at a level where boards can make prioritisation and investment decisions.

From our own experience with UK clients there appears to be a general tension between the services firms have chosen as important business services and those they would identify to actually run their business. Many firms have selected only "paying claims" as an important business service. While this might meet the regulatory requirements, it

[5] Bailey, D. (4 May 2022). Speech: Operational Resilience – Next Steps on the Prudential Regulation Authority's Supervisory Road Map. BIS. Retrieved 23 October 2023 from https://www.bis.org/review/r220502e.htm.

is worth considering if it is sufficient to be a truly resilient organisation. An exercise to think more broadly about the services that are offered by the firm may provide better outcomes when a disruption does occur.

In an Irish context, similar issues have arisen. Despite there being a clear definition within the CBI guidance of what is meant by the term "critical or important business service," there still appears to be some confusion over what it means in practice. In some cases, there is confusion between processes and services when determining the list of critical or important business services. For example, some firms have listed key processes which would normally underpin the delivery of such services rather than being critical or important business services in their own right. For example, policyholder communications process may be incorrectly designated as a critical or important business service.

In other instances, the identified critical or important business service is not so much an individual service but a whole collection of different services. For example, an identified critical or important business service may be described as "all policyholder servicing and administrative activity," which, of course, will comprise a whole range of different services to policyholders, many of which will have varying levels of importance and varying tolerance limits in the event of an operational disruption.

In some cases, there has also been a lack of clarity in relation to how to apply board-approved selection criteria in order to identify a firm's list of critical or important business services. In particular, where there are a number of criteria, it is unclear whether or not a given service merely needs to satisfy one of these criteria or needs to satisfy multiple (potentially all) criteria. It is also unclear what threshold needs to be reached before a given criterion has been satisfied. For example, if one of the criteria for assessment of a service as being critical or important is the impact on the firm's stability or financial soundness, then there needs to be some form of measurement scale applied in order to determine the extent to which each service being assessed impacts the firm's financial stability or financial soundness.

Critical infrastructure

In many instances, the delivery of critical or important business services will depend on the availability of critical national infrastructure, such as payments through BACS. While this issue has not yet come to the fore in an Irish context, many firms in the UK are struggling with this dependency in the context of operational resilience, as it partially takes control away from a firm with regard to being able to meet impact tolerances in the event of a disruption. The regulatory authorities seem to be comfortable with this dependence though (i.e., on national infrastructure) as they appreciate that individual firms can't really do much about it. That being said, in order to achieve operational resilience, if a firm deems that the ability to pay claims is critical or important and the BACS system fails, then it will still need to have a plan in order to ensure that customers do not suffer intolerable harm. In the UK this has led to some early thinking by the regulators about designating certain third parties (e.g., cloud providers or administrators) as critical outsourcers and putting particular conditions on them.

Impact tolerances

On impact tolerances David Bailey commented that, for those firms that had been assessed, more progress had been made at the time on important business services compared to impact tolerances. In part this was due to impact tolerances not being set to meet the objectives of both regulators (with the PRA being focussed on firms' safety, soundness and financial stability, with the FCA being focussed on customer harm and market integrity). As a result of the wide range of granularity identified in important business services, impact tolerances also demonstrated a wide range of tolerable outcomes. As a result, Mr Bailey mentioned that future supervisory reviews on the topic would focus on justification of the level at which impact tolerances are set and more detailed reviews across peer groups. Furthermore, he noted that this is an area where "dialogue amongst the industry would be beneficial to share information on the various approaches taken to modelling and setting impact tolerances."

In an Irish context, many firms' choices of impact tolerances are not being supported by detailed examinations of what is meant by intolerable harm and when it might begin to arise. This can result in tolerances being set at a very generous level before it is deemed that an intolerable harm would arise. It also results in a very narrow set of criteria being used for tolerance limits. The CBI specifies that "at a minimum, there should be a time-based metric indicating the maximum acceptable duration a critical or important business service can withstand a disruption." Many firms do not look beyond a time-based metric, however, and can therefore miss other important indicators of when intolerable

harm may be about to occur. In addition, there can often be confusion between risk appetite and the concept of impact tolerance associated with operational resilience, which further compounds issues related to the setting of appropriate tolerances.

Process mapping and scenario testing

In a letter to firms dated March 2023, the Bank of England and PRA communicated the findings of a cyber stress test which had been conducted in 2022. Commenting specifically on operational resilience, the letter stated that "firms will be expected to show that they are testing against severe but plausible scenarios, such as the one used in the 2022 cyber stress test, and this testing should become more sophisticated over time. Firms are expected to demonstrate through testing, that they are able to remain within impact tolerance or, when they are unable to do so, to invest and take action to improve their operational resilience."[6]

Scenario testing is a key feature of operational resilience preparedness and is required by the CBI guidance. To be useful, though, scenarios must avoid just focussing on single points of failure (in a way similar to how business continuity or disaster recovery scenarios might), but rather be holistic in nature, aimed at testing the vulnerabilities in the delivery of a given service as a whole, and testing the firm's ability to remain within its desired impact tolerance. In many cases, scenarios are not severe enough to properly test impact tolerances because the situation is assumed to have been remedied before the defined impact tolerance has been surpassed.

One of the aims of process mapping is to facilitate the identification of key dependencies in the delivery of critical or important business services—in particular where they involve external third parties, or where there is interconnectedness between the people, processes, systems and locations underpinning the delivery of different critical or important business services. These maps must be sufficiently granular to allow this to be possible. However, this is not often the case. In many instances, process mapping does not include any overview of the various steps involved in the delivery of each service, i.e., a simple process flow illustrating all of the key activities along the way. Furthermore, while there are process maps supporting each individual service, many firms have not looked across the range of services to see where the interconnectedness arises (if, indeed, it arises at all).

Self-assessment

The Bank of England and PRA further communicated that they "expect to see the testing and remediation workplan that provides board-level assurance that the firm will be able to remain within impact tolerances. These should be included in firms' self-assessments."

Although still at a very immature stage in Ireland, the self-assessment exercise (which is an important component of a well-functioning operational resilience framework) is sometimes seen as a compliance exercise, i.e., focussed on assessing whether or not each aspect of the CBI guidelines has been adequately addressed by the operational resilience framework, as opposed to being an objective assessment of the overall state of operational resilience at the firm (having taken into account scenario test results, lessons-learned exercises and any remedial actions that need to be taken in order to improve resilience).

Shared ownership

Effective implementation of an operational resilience framework requires input from many different stakeholders. Therefore, it is imperative to involve people from right across the business in developing the criteria for selection of critical or important business services, developing the associated process maps, setting impact tolerances, conducting scenario testing and, especially, carrying out comprehensive lessons-learned exercises. Without general buy-in from different functions within the company it is not possible to properly identify and address vulnerabilities. In many firms, we see operational resilience being handled by a small number of people, mainly representing operations and risk management, without input from across the business.

[6] Bank of England & PRA (29 March 2023). Thematic Findings From the 2022 Cyber Stress Test. Retrieved 23 October 2023 from https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test.pdf.

In summary

It is clear that firms both in the UK and Ireland have come a long way on their operational resilience journeys. The industry in Ireland can learn from some of the experiences of UK firms due to their relative positions on these journeys and the insightful feedback and commentary that has been shared by the regulatory authorities. With a looming implementation date of December 2023, firms in Ireland will soon need to be "in a position to evidence actions/plans to apply the Guidance" issued by the CBI. By taking on board the experiences of the industry in the UK it may be possible for Irish firms to accelerate the effective implementation of their operational resilience frameworks.

Milliman

CONTACT

Adél Drew
adel.drew@milliman.com

Eamonn Phelan
eamonn.phelan@milliman.com