Operational resilience: Navigating the new requirements

Milliman

Introduction

In its *Cross Industry Guidance on Operational Resilience*, the Central Bank of Ireland (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.*" In addition, to become operationally resilient, a firm must be able 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.*" This can range from the ability to bounce back from a relatively minor disruption to being able to seamlessly continue to deliver key services during a period of sustained and transformational change.

The publication of the CBI guidelines last December has prompted the insurance industry in Ireland to formally consider its operational resilience, and different firms are at different stages on that journey.

Operational resilience in context

Operational resilience is clearly important, but how does it differ from operational risk management? In the first instance, operational risk management is concerned with a much broader range of potential issues than purely disruptive events. If we just consider disruptive events though, operational risk management focusses on identifying what can go wrong, measuring the potential impact, developing and implementing mitigating controls and communicating with key stakeholders. It attempts to avoid or to minimise the likelihood of adverse events actually occurring at all. Operational resilience, on the other hand, considers disruption inevitable. It demands that we understand the firm's business and the key steps and activities needed in order to consistently deliver upon its key commitments in the form of the critical or important business services that it provides.

Firms must be able to continue to deliver these services in the face of the challenges which are presented when things do not go to plan, and to do so in a manner which portrays a very calm, business-as-usual exterior. It is much more than just disaster recovery (DR) or business continuity management (BCM). It is about withstanding, responding and adapting to whatever set of circumstances arises and emerging stronger than ever. Taken together, operational risk management and resilience can help a firm to recognise operational risk exposures and do all within its power to mitigate or avoid them, while at the same time being fully prepared for those events which will inevitably materialise.

This requires a unified approach across the organisation, with coordinated effort from risk management and operations in particular, drawing together existing processes such as business continuity management, recovery planning, outsourcing oversight and cyber risk management, amongst others, to arrive at a holistic view of the firm's exposures and capabilities.

The Three Pillars

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:

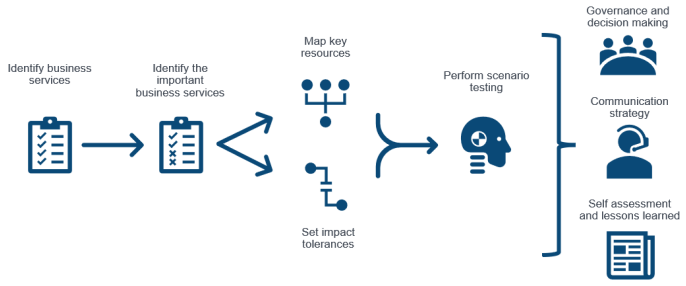
- Identify & Prepare
- Respond & Adapt
- Recover & Learn

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 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 key components of the overall fabric of an operationally resilient firm and must be brought together to help deliver the desired outcome.

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.

Figure 1: The Operational Resilience Process



These 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. The CBI also mentions the proposed new EU legislation in relation to digital operational resilience known as the Digital Operational Resilience Act.

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.

Challenges

There are a number of significant challenges to overcome on the journey to becoming an operationally resilient firm. Addressing these challenges will require varying degrees of effort across different firms, depending on their individual circumstances, the nature and complexity of their operational processes and their general state of readiness.

Identifying the critical or important services

A cornerstone of operational resilience is to first identify the firm's critical or important business services, using a board-approved set of selection criteria. Arriving at a suitable and robust set of criteria, certainly first-time through the exercise, can be quite a daunting task. While the CBI does not offer much guidance on the criteria themselves, the FCA is quite clear in what it sees as the considerations to bear in mind, as listed below. This may help to provide a good steer for firms seeking to put such criteria in place.

- The nature of the client base, including any vulnerabilities that would make a person more susceptible to harm from a disruption
- The ability of clients to obtain the service from other providers (substitutability, availability and accessibility)
- The time criticality for clients receiving the service
- The number of clients to whom the service is provided
- The sensitivity of data held
- Potential to inhibit the functioning of the financial system
- The firm's potential to impact the soundness, stability or resilience of the financial system
- The possible impact on the firm's financial position and the potential to threaten the firm's viability, which could harm the firm's clients or pose a risk to the soundness, stability or resilience of the financial system or the orderly operation of the financial markets
- The potential to cause reputational damage to the firm, where this could harm the firm's clients or pose a risk to the soundness, stability or resilience of the financial system or the orderly operation of the financial markets
- Whether disruption to the services could amount to a breach of a legal or regulatory obligation
- The level of inherent conduct and market risk
- The potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure
- The importance of that service to the financial system, which may include market share, client concentration and sensitive clients (for example, governments or pension funds)

Another one of the initial key challenges is to formulate, and then communicate, a single unified view of the overarching operational resilience framework across the organisation. This framework will have many touchpoints and interlinkages with existing risk management and governance processes across the organisation, including, amongst other things, risk appetite, preemptive recovery planning, business continuity management, outsourcing oversight and governance and operational risk management.

Risk appetite

The firm's appetite across a range of different metrics (from reputational risk to operational risk losses to persistency, for example) should help to form a view of its implied appetite for operational discontinuities. This should help to inform, and ultimately bear a close similarity to, the tolerances for such discontinuities that are required as part of the CBI's guidelines.

However, care is needed, as oftentimes the firm's risk appetite can be somewhat inward-looking in nature, i.e., in some instances it is more concerned with matters which are of importance to internal stakeholders rather than external stakeholders. The requirements and expectations of these two groups may not always be aligned when it comes to operational resilience.

Therefore, it may be necessary to use some aspects of risk appetite to guide the firm's tolerance for disruption to its critical or important business services, while potentially using these same tolerances to recalibrate risk appetite in other areas. For example, the firm may have a particular risk appetite for persistency risk. From an operational resilience standpoint, the firm may wish to limit the impact of any disruption to its ability to service its policyholders by building spare capacity into its processes.

However, this may be at odds with its appetite for expense risk, potentially leading to a need to accept more risk in this area.

Recovery planning

Preemptive recovery planning considers, amongst other things, the potential impact on the operational capacity of an organisation when assessing the wider implications of implementing a given recovery option. For example, if a recovery option involves the disposal of a business unit which delivers a key service to another part of the organisation, then this could lead to an unintended disruption to the delivery of the firm's critical or important business services. Identifying the key dependencies is a crucial part of the operational resilience framework and, once identified, these key dependencies should be appropriately reflected in recovery plans. Similarly, useful insights may be gleaned from some of the recovery scenarios which are included in preemptive recovery plans when it comes to scenario testing within the operational resilience framework.

Business continuity management

In the words of the CBI, traditional BCM "*focuses on single points of failure, such as individual systems, people or processes.*" It also tends to focus on getting back to business as usual in the context of how the business looked prior to the disruption. It can be considered to be quite short-term in nature, i.e., a rapid response to a particular pain-point, aimed at restoring service to business as usual. The requirements of operational resilience are much broader though. Ideally, within a fully resilient organisation, BCM should never actually be needed.

However, if the response to a disruption necessitates invoking business continuity plans, BCM will need to be built out to include, amongst other things, crisis management, impact analysis and ongoing training of key personnel. It also needs to consider how business continuity can be maintained during periods of upheaval which might not result in the circumstances of the firm returning to the same state as existed prior to the upheaval occurring in the first place. In effect, BCM needs to be much more holistic in order to achieve the aims of operational resilience.

Outsourcing

Depending on its extent and overall level of complexity, outsourcing can act to reduce visibility in relation to a firm's ability to continue to deliver critical or important key services. When mapping how its critical or important business services are delivered, a firm needs to "*identify, document and map the necessary people, processes, information, technology, facilities, and third parties service providers*" which form part of each service delivery.

In explicitly mentioning third parties, this definition bears striking resemblance to the requirements of the both the PRA and FCA in the UK. When involving third parties in the delivery of a critical or important business service, a firm is effectively now relying on the operational resilience of that third party. This is something that needs to be properly assessed as part of the initial and ongoing due diligence, which needs to be undertaken when entering third-party arrangements in order to ensure that the third parties in question are sufficiently resilient to enable the firm to remain within its own impact tolerances. Importantly, the scenarios which may cause an operational issue for a third-party service provider may not be the same as those scenarios which may trouble the firm itself, and any such mismatches should be explored and understood.

Scenario analysis

It can sometimes seem as if there is an almost never-ending list of scenario testing requirements that firms must satisfy. In addition to the Own Risk and Solvency Assessment (ORSA) and firms' preemptive recovery plans, as well as (in some cases at least) internal assessment of operational risk capital requirements, the CBI's guidance in relation to scenario testing for operational resilience expects firms to "*identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the firm's critical or important business services in those circumstances.*"

There are synergies to be gained through careful scenario selection. Choosing scenarios which tell a more comprehensive and coherent story can, potentially, be used for multiple purposes, thereby creating a stronger and clearer message for key stakeholders. It allows them to see and understand the implications through a range of lenses, from capital requirements through to operational resilience, and importantly also serves to reduce the resource demands associated with such analyses.

Further considerations

There are many further challenges to tackle and overcome on the way to achieving operational resilience, including setting impact tolerances, i.e., what is the maximum acceptable level of disruption to a given critical or important business service? These challenges, in turn, need to be tested against a set of severe but plausible scenarios.

There are significant documentation requirements associated with the CBI's guidance, and producing it to an acceptable standard will, in itself, be no small task. While there will inevitably be a significant effort required to put everything in place initially, further effort will be required in order to properly embed operational resilience best practices across the firm, and to conduct the key aspects of the process on an annual basis to ensure continued fitness for purpose.

Given that the industry is, in general, seeking to address these requirements for the first time, it can be quite difficult for individual firms to identify best practices and to ensure that they keep abreast of others. It can therefore be beneficial to seek input either from elsewhere within the group (if applicable, and if other parts of the group are located in jurisdictions which have implemented their own operational resilience frameworks), or to seek input or review

from external parties who can offer insights into emerging best practice.

Implementation timeframe

The CBI has stated that it expects firms in Ireland to be actively and promptly addressing any existing operational resilience vulnerabilities that they have identified and to "*be in a position to evidence actions/plans to apply the Guidance*" (i.e., the CBI's operational resilience guidance) by December 2023.

Our experience in the UK market (which is already quite well-advanced in the implementation of operational resilience requirements) is that initial phases of preparation can take up to six months to complete. This involves the identification of critical or important business services and creating the process maps associated with them. It can take a year—and perhaps longer—to work through the remaining requirements and to begin to address vulnerabilities. While the CBI deadline is still approximately 18 months away, some firms still face quite a body of work in order to meet this expectation.

Next steps

Understanding the gaps between the current state and the desired future state as regards operational resilience is a critical next step. Many firms have already commenced such analyses, with others still in the planning stages. Understanding the full extent of the effort required and allocating resources accordingly will afford firms the best chance of satisfying the requirements of the guidance.

Milliman

CONTACT

Eamonn Phelan

eamonn.phelan@milliman.com