OPERATIONAL RESILIENCE:
WHAT LESSONS CAN BE LEARNED FROM THE FIRST ROUND OF SCENARIO TESTING?

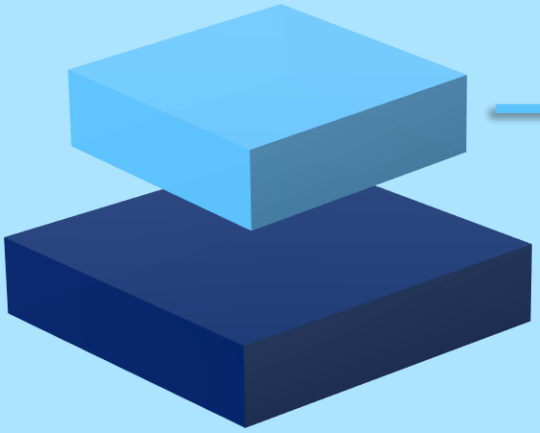
On the 31st of March, the PRA/FCA's landmark Operational Resilience Policy will come into full force. In effect, this means that, in just a few weeks, all large UK financial institutions will be required at the very least to have

- identified their **important business services** (IBSs),
- mapped the resources (people, property, third parties, data, technology) to each of their IBSs,
- set associated **impact tolerances** for each IBS at the point where disruption would cause intolerable harm to customers, or the financial stability of the firm, or wider market,
- begun testing their ability to stay within impact tolerances using **severe but plausible scenarios**,
- document methodologies, results, and next steps in their self-assessment,
- begun remediation of identified vulnerabilities to be completed by March 2025,
- started putting this plan into action.

Firms are at a variety of stages along their compliance journey and have taken a range of different approaches to the definition of IBSs, mapping of resources, setting of impact tolerances, and scenario testing.

Over the last year, Beyond Blue have been hard at work consulting with our clients in the financial sector with a particular focus on developing and implementing comprehensive and robust scenario testing programmes. In this Bulletin, we share some of the key lessons we have learnt from this process.

OUR APPROACH TO SCENARIO TESTING



TIER 1

IBS SPECIFIC TESTING

Informed by resource mapping, we develop a range of unique scenarios for testing each IBS.

TIER 2

INFRASTRUCTURE TESTING

Where mapping has identified resources that are critical to multiple IBS, infrastructure scenarios are used to test foundational infrastructure, critical applications, third parties and severe cyber scenarios.

Beyond Blue's approach to scenario testing for Operational Resilience separates scenarios into two buckets. The first bucket is made up of scenarios designed to test whether individual IBSs can remain within their impact tolerances. The IBS-specific scenarios are developed using the resources that have been mapped to each IBS and are understood to be critical to the availability and integrity of that IBS. The second bucket comprises scenarios designed utilising resource mapping to identify critical assets that support multiple IBSs and included scenarios focused on critical business infrastructure, zero-day ransomware and third-parties.

IBS-specific scenario testing enables a firm to test scenarios that range in severity, to help identify scenarios where they can remain within impact tolerance as well as identify those where they cannot. IBS-agnostic scenario testing allows a firm to identify more severe scenarios that require firms to coordinate recovery of multiple IBS, often simultaneously. Testing using both forms of scenarios helps firms achieve a more robust and durable form of resilience than is possible focusing merely on testing IBS-specific scenarios. Using this approach, here are some of the key lessons we've learned.

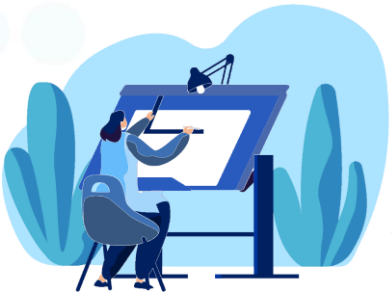
LESSON 1: YOUR SCENARIO TESTING WILL ONLY EVER BE AS GOOD AS YOUR RESOURCE MAPPING

Reliable and accurate resource mapping is key to effective scenario testing. To ensure that the scenarios you design can provide you with meaningful outputs, it is vital to have up-to-date and appropriately detailed view of the **resources essential to the availability and integrity** of those services; along with a view of their upstream and downstream dependencies. This mapping will be a key input into scenario development in helping identify single points of failure and modelling impact. When testing infrastructure scenarios, understanding the "handshake" between IBSs and underlying infrastructure is critical to understanding the recovery dependencies. This task can be challenging. But it is not an area where you want to cut corners. The use of inaccurate resource maps will lead to unreliable results, however thoughtfully constructed your scenarios and well-managed your exercising. The consequence of this will be your organisation harbouring a misplaced confidence in the resilience of your IBSs and the underlying infrastructure.

LESSON 2: YOU NEED TO GET CLEAR ON WHAT IT MEANS TO SAY A RESOURCE IS "CRITICAL" TO THE DELIVERY OF AN IBS

Resource mapping involves determining which aspects of your organisation are "critical" to the delivery of an IBS. It can be tempting to seek a crisp definition of criticality in terms of quantifiable metrics. This temptation should be avoided. The regulations are clear that resources should be identified as critical where, if rendered unavailable or where their integrity is lost, this would disrupt the successful delivery of the IBS to **1 or more** customers. This is a very low threshold. It is vital that you and your team remain alert to this fact and this definition of criticality is understood and applied consistently across the organisation. It is easy to backslide into using volumetric thresholds to define criticality over time leading to a concept of acceptable customer harm, especially given the tendency of many to automatically assume a risk-based approach to thinking about resilience (see lesson 4). Make sure this definition of criticality is well understood and at the very heart of your implementation program. Challenge yourself to have the interest of all clients and customers in mind.

LESSON 3: TESTING CAN HELP A FIRM UNDERSTAND THE TRULY CRITICAL IBS, INFORM RECOVERY SEQUENCING AND DEFINE THE MINIMUM VIABLE BANK



The primary function of scenario testing for operational resilience is to determine whether an IBS is within its impact tolerance. Consequently, the focus in designing scenarios is primarily placed on IBS-specific scenarios which enable structured stress testing of critical resources specific to that IBS. However, aggregating and analysing the mapping outputs to identify concentration risk across your IBS can prove valuable and inform the development of infrastructure scenarios. Well-designed scenarios in this category can provide vital information about interdependencies between IBSs and a deeper, architectural understanding of the resources supporting them. This information can be hugely valuable to how you think about recovery strategy. In part--icular, it can help you to identify the IBS recovery priorities which would best mitigate intolerable harm in the case of an organisation wide incident impacting the majority or all IBSs. Good examples of this would be ransomware and major data corruption scenarios. These can help identify the critical sets of IBS which must be restored first and associated infrastructure rebuild sequences. This knowledge can then be used to inform any architecture redesign required to ease the prioritised recovery of these IBSs in a timely manner, as well as informing the design of customer treatment and substitutions needed during the recovery of those systems.

WHAT TO DO ABOUT THIRD PARTIES

The responsibility of assuring the security and resilience of financial market infrastructure (FMIs) and other sector-critical third parties has been a point of contention between the regulators and financial institutions, long before the release of the Operational Resilience Policy. Whilst previous sector-wide third-party assurance efforts between firms have seen vary--ing degrees of success, the operational resilience policy presents an opportunity for alignment in approach across the industry. The benefits of this will be two-fold.

a) For the third parties it will reduce the overhead of responding to multiple requests that are generally asking for the same thing.
b) This in turn will encourage third parties to provide more detailed, evidenced responses to a single request in order to satisfy the majority of firms. Ultimately, this will provide firms with more assurance over a group of systemically important FMIs and third parties.

The multiple industry-wide information sharing forums are the ideal vehicle to drive such sector-wide initiatives, and provide a safe space for firms to collaboratively produce a standardised methodology and approach.

LESSON 4: MINDSET SHIFT FROM RISK TO RESILIENCE

Perhaps the most significant cultural challenge to the implementation of the Operational Resilience Policy has been a tendency of some to take a risk-based approach (i.e., one which assumes that the preventative controls firms have invested in for many years reduce the likelihood of severe but plausible scenarios taking place)**.** It is not just that regulatory guidance warn against conflating risk and resilience.[1] Ultimately, adopting a risk-orientated mindset is liable to result in resource mapping and scenario design which unduly prioritise some resources and outcomes over others based on considerations of likelihood. This can mean scenarios which demonstrate that you are not within your impact tolerances may be overlooked. For this reason, it's vital to ensure that those involved in your implementation programme understand this shift in emphasis from a risk-focused to a resilience and recovery mindset. There needs to be broad agreement that, **whilst scenarios may seem low probability they remain plausible and multiple controls can and do fail – and are therefore worth considering from a recovery perspective.**

LESSON 4 CONTINUED

The best example of this would be to rewind the clock back to 2015 before the explosion of ransomware. The tendency to focus on risk is understandable; it has been the favoured approach for many years. Firms have invested heavily in preventative functions, none more so than Cyber. To ask subject matter experts (SMEs) to not only invest in preventing these scenarios materialising but at the same time, disregard the likelihood reducing capability of these preventative controls and invest in recovering from these scenarios, is not something that can be achieved overnight. But ultimately multiple controls do fail in surprising ways and common failure modes and root causes can be ignored. Balance a protective mindset with an investment to build a response and recovery capacity.

LOOKING TOWARDS TO THE NEXT ROUND

Post March 2022, the regulators will inevitably hunker down to digest and analyse each firm's approach in turn. We can expect them to resurface in late 2022 or even 2023 with a general position of good practice. In the meantime, here are a few areas for firms to focus on:

- ***MOVE TOWARDS MORE IBS-AGNOSTIC PROCESS MAPPING AND SCENARIO TESTING***

Many firms will now have completed resource mapping and conducted testing several scenarios. Consequently, they should have a fairly good read on the direct dependencies between their critical resources and IBSs. They may have also identified IBSs which exceed their impact tolerances and begun the necessary remediation work. As their compliance program progresses to the next stage, this focus will need to shift towards infrastructure scenarios and more complex data integrity and cyber scenarios. Whilst the volume of scenario testing will decrease, the **depth of analysis required to accurately identify IBS specific impacts, recovery processes, timelines and customer harms will increase**, especially if the mapping outputs do not provide sufficient detail.

- ***THE VALUE OF SCENARIO TESTING***

To ensure scenario testing continues to deliver value, there are two questions to ask as each new scenario is developed: (1) "**Will the scenario provide a new perspective on potential failures and their client impact?**" and (2), **"Is the scenario likely to identify new vulnerabilities or potential recovery requirements?**" Given the size and complexity of many UK financial institutions, answering these questions can be a challenge. Various parts of the firm will often be undergoing transformation programs at any one time. Hence, to benefit both testing and remediation, it is key to ensure visibility over all existing transformation programs, leveraging and plugging into existing governance structures where possible to do this. Whilst coordination of this scale is complex, the benefits are obvious: avoidance of wasted resources on scenario testing known vulnerabilities, avoidance of duplicative effort to remediate vulnerabilities, and a chance to shape existing transformation programs to embed resilience thinking early on.

- ***TENSIONS BETWEEN RESILIENCE AND OTHER ORGANISATIONAL OBJECTIVES WILL INTENSIFY***

Various objectives of your organisation will likely increasingly find themselves at odds with those of your operational resilience programme. The simple reason for this is that **measures which you take to optimize your systems and reduce risk might make your firm less resilient**. E.g., reducing the number of data centres also introduces fewer, more concentrated points of failure but perhaps design in better recovery processes. Continuing to provide an IBS after an incident might increase your firm's risk profile if you are forced to disable security or fraud controls to restore service. These tensions and discussions are constructive and important, and not to be avoided.

FINAL THOUGHTS

The regulators intention with the Operational Resilience Policy was to force firms to move away from focusing on purely preventing incidents to learning how to live with them. In the last five years, the impact of Cyber incidents has increased exponentially, the world is slowly recovering from a two-year pandemic and at the time of publishing in March 2022 we are focused on events in the Ukraine. The regulator's timing was spot on – and resilience seems more important than ever.

[1] See S21/3: Building operational resilience (FCA), Annex 2, §6 and PS6/21 (PRA) §§4.29-32, 6.6