Operational Resilience

5 things not to tell your regulator

By JADEtc.

For a decade, operational resilience has been a major focus of global and national regulators. By *resilience*, regulators don't mean to invent a new risk type or risk category; operational resilience is the **outcome of effective operational risk management**. In the UK, regulators published final policy in 2021 which provides a detailed rules and guidance for delivering on their expectations. Many other national regulators have also published their own policies in line with the Basel Principles for Operational Resilience 2021.

Firms in the UK have until **the latest end March 2025** to have implemented the rules and to be confident they can remain within impact tolerances given severe but plausible operational disruptions. Regulators have intensified their scrutiny of firms' approaches and this will only increase during the next year. When the regulators come knocking, how will you respond? Here are 5 things **not to tell** your regulator in relation to operational resilience.

One: Vulnerabilities due to third (and fourth) parties aren't our problem

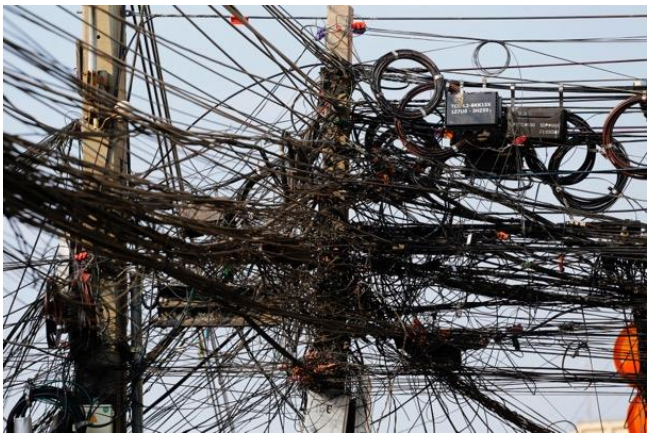
In the UK, regulators published new rules and guidance on third party risk management at the same time as they issued the new rules on operational resilience and they emphasized the importance of robust third party risk management for achieving the desired resilience outcomes.

The new rules – set out in **SS2/21** – provide prescriptive rules and guidance on the lifecycle of outsourcing, including procurement, materiality and risk assessments, ongoing due diligence, exit strategies and testing, and the approach to 4th parties. Regulators have also

broadened the scope of coverage to include **non-outsourcing third party arrangements** and reiterated that **intra-group outsourcing** should be treated the same as outsourcing to external third parties.

What has not changed, is that regulators will hold the firm (and its Board of Directors) **accountable** for all activities, even those outsourced to third parties. As the mantra goes, you can outsource *the responsibility* but not the *accountability*.

It's therefore vital that vulnerabilities to resilience arising from third parties are identified promptly and action taken to mitigate them – including through identification of recovery options and 'plan bs'.



Two: We're using our operational risk scenario testing for operational resilience

A key activity in delivering resilience is to test Important Business Services (IBS) with severe but plausible operational disruptions to determine whether services can be recovered within established impact tolerances. For many aspects of delivering operational resilience, firms can leverage existing tools and frameworks (e.g. of operational risk management). However, in the case of scenario testing, this is not likely to be sufficient.

There are several key differences between traditional scenarios for operational risk management and those for operational resilience.

First, scenario testing for operational resilience is more akin to reverse stress testing than traditional scenario testing for operational risk. Firms must test their ability to continue delivering an IBS in the face of disruptions of increasing severity to the critical resources required to deliver them. Severity of the disruption should be increased by extending the duration of the disruption (beyond the impact tolerances) and by adding disruption to additional critical resources. It's vital that the tests challenge the firm and make it consider alternative means of delivering services rather than merely to confirm everything is fine.

Second, the scenario storyline, important for operational risk testing, is not important for resilience testing as the cause of the disruption is immaterial. It's useful to have a storyline to help participants, for instance how the corruption of critical data occurred, for instance due to a cyber attack, but this is a minor feature of the test and shouldn't be a major focus for discussion.

Third, unlike in operational risk scenarios, the **likelihood** of the disruption is **irrelevant** in operational resilience testing. The testing must assume a likelihood of 1, in other words it assumes the disruption has occurred and preventative controls have failed. This helps avoid debates in resilience workshops about *what could be done to prevent the incident* or of people claiming '*this couldn't possibly happen to us'*. Firms must *assume* disruption to the critical resource(s) has occurred – as long as it's plausible – and then test their ability to recover and adapt to remain within impact tolerances.

Of course, the testing done for operational risk management and business continuity management can be a useful input to resilience testing, but to simply relabel the other types of testing won't cut the mustard when it comes to meeting regulatory expectations on resilience.

Three: Our impact tolerances for UK regulators PRA and FCA are the same

A key component of the UK regime is for firms to set **impact tolerances** related to customer harm, firm safety and soundness, market integrity and for systemic firms financial stability. All firms are required to set tolerances related to duration, but firms have also recently been encouraged, in a thematic letter to firms, to consider whether tolerances other than duration may be appropriate e.g. related to the number of vulnerable customers impacted.

Some firms have set tolerances for consumer harm and firm safety and soundness the same. Regulators have provided feedback that this is not appropriate, and different tolerances should be set for both. Setting tolerances for consumer harm – which will typically be a matter of days – the same as for a risk to firm safety and soundness, may also raise eyebrows at the regulator that an operational disruption could result in a threat to the firm's safety and soundness in such a short duration and might provoke a review of their ICAAP and ILAAP!

Four: The COO / SMF24 are dealing with operational resilience

UK regulators are increasingly holding specific individuals to account for key elements of regulation and operational resilience is no exception. The COO or SMF24 (the COO

function under the Senior Managers and Certified Persons Regime) should be responsible for **implementation** and **reporting** on operational resilience.

In many firms, a pragmatic approach, especially given a relatively challenging initial deadline at end March 2022, was for the COO/ SMF24 to take the lead on design of the framework and in many cases ownership of the operational resilience policy. Although this was fine as an initial approach, it's clearly not appropriate for the same 1st line function to own both the policy and be responsible for its implementation. More properly, the operational resilience policy should be owned in the 2nd line and the 1st line should focus on implementation and reporting only. Many firms are making the adjustment and it's likely regulators will scrutinise roles and responsibilities and proper segregation of duties across the 3 lines.

Five: There's plenty of time to the deadline – I don't need to worry about this yet!

UK regulators are not known for providing long implementation periods for new rules, especially post the GFC. However, on operational resilience, UK regulators have given firms 4 years from the publication of the final rules in March 2021 to the final implementation deadline of end March 2025.

However, the reason for the long implementation period is not driven by their generosity. Regulators introduced the new rules because they were dissatisfied with the resilience of firms, who too frequently were unable to continue providing services when they suffered operational incidents – the TSB IT meltdown being the more egregious example – and as such caused harm to consumers, damaged firm safety and soundless and the integrity of the market. Regulators anticipate that firms will need to **take actions** to address these vulnerabilities and these may include replacing obsolete systems or replacing critical third parties. Implementing new systems and replacing vendors takes time, and this is the reason for the long implementation period. Telling regulators that you're waiting until the last minute to identify vulnerabilities that may then not be addressed by end March 2025 will undoubtedly raise significant concerns and is a sure-fire way to a S166 or worse.

****