A Year In Operational Risk and Some Reasons To Be Optimistic

To borrow an expression from HRH Queen Elizabeth's Christmas Speech of 1992, 2020 was an '*annus horribilis'*. And to quote the rock band Queen, 'These are the days it never rains but it pours'. 2020 was an awful year and there was a rare consensus that the sooner it was over the better! However, for Operational Risk Management (ORM) we believe there are some positives that can be taken from 2020 and what's more, there are reasons to be optimistic for the future. We've identified 5 reasons that we explore below.

1. Continuity of service during Sars-Cov19

The pandemic dominated 2020, causing enormous disruption, both direct and indirect via the responses of governments to the crisis. Many firms had pandemic on their risk register since at least 2006, when the UK regulator did its market-wide exercise on an avian flu pandemic. However, no firm could have anticipated the full impacts, including in particular the use of 'lockdowns', of the 2020 crisis. Although pandemic risk was certainly not a 'Black Swan', the lockdown response was unimagined before last year.

However, for the most part, firms' appear to have maintained continuity of operations, in many cases transforming their operations to be entirely based on home working. So far, there have been no major operational risk events reported publicly (albeit this may be due to remote working weakening detective controls) and there is anecdotal evidence that firms have used their ORM tools to good effect (many doing ad hoc RCSAs to identify heightened areas of risk and putting in place mitigating controls).

2. Regulatory focus on Operational Resilience

The events of last year have provided a real-life stress test for firms in relation to their resilience, and many appear to have coped well. But as PRA's Nick Strange made clear in his speech at Op Risk Europe 2020, firms should not be complacent. Future events may be very different in nature to the challenges of Sars-Cov19, specifically they may be more idiosyncratic in nature (Sars-Cov19 impacted all firms) and may emerge with greater velocity (in contrast to Sars-Cov19 which emerged over several months giving firms time to prepare). The fact that everyone was in the same boat last year also meant that consumers tended to be more tolerant of poor service, that might otherwise have drawn considerable ire.

Following the Global Financial Crisis, regulators focused on financial resilience requiring more capital and more liquidity. In more recent years, they've turned their attention to operational resilience and in the last year we've seen consultation papers from national regulators (including in the UK and US) and from the Basel Committee on Banking Supervision.

Although initially there was some confusion on what this meant (Was it a new risk type? Was it a new name for business continuity?), regulators have subsequently been clear that operational resilience is an **outcome** of **effective operational risk management**. As the Bank of England's Lyndon Nelson told a conference of operational risk managers in 2019, the regulatory focus on operational resilience provides an **exciting opportunity** for operational risk management as a discipline and for operational risk managers as the practitioners:

> *Recently I was asked to say a few words to a group of new Operational Risk managers. I told them that they would be pioneers. I foresaw that operational resilience would be seen to be on a par with financial resilience and a key part of a firm's risk profile. I felt that this would be transformational for many organisations. So an exciting time? Yes, but operational resilience is hard.* (Resilience and continuity in an interconnected and changing world, Speech given by Lyndon Nelson, Deputy CEO, Executive Director, 20th Annual Operational Risk Europe, 13 June 2018)

A primary reason for the regulatory focus on operational resilience is that too many firms had palpably failed to achieve the required level of resilience (in line with the risk tolerance of regulators), leading to several well publicised scandals. These in turn led to a UK Parliamentary Inquiry on *IT failures in the Financial Services Sector* which was published in October 2019 and which made a number of recommendations which regulators then acted on.

Regulators in the UK are expected to finalise proposals for operational resilience in first quarter 2021 which will be implemented over the subsequent 12 months, and firms are expected to be given up to 3 years to become fully resilient. Many firms will need to review and enhance their ORM frameworks in order to meet the raised regulatory expectations on resilience and get on a W.A.R. footing – able to Withstand, Absorb and Recover from disruptions without causing intolerable harm to consumers, markets, the firm's safety and soundness and the overall financial system.

3. Turning the tide on fragmentation

One of the reasons for the failure of ORM to deliver adequate levels of resilience was that it had become fragmented. After the Global Financial Crisis, regulators focused on 'conduct' and many large firms established new conduct risk functions and frameworks. Since then, many firms also established separate risk frameworks for financial crime, cyber risk, business continuity and so forth. New frameworks grew like Topsy, adding to complexity, confusion and inefficiency!

There were signs in the early discussions on operational resilience that firms were destined to repeat the mistakes of conduct, and that ORM would become even more fragmented with new resilience risk functions and frameworks. Thankfully, regulators clarified that they expect firms to utilise existing ORM tools to deliver resilience, and the risk of further fragmentation

seems to have been averted. To deliver operational resilience efficiently, firms should develop integrated ORM 'umbrella' frameworks, that provide a common approach (governance, language, taxonomy, tools and so forth) across the various components of operational risk. The new elements (e.g. resource mapping, impact tolerances) should become new components of the ORM toolkit.

4. Human Risk comes to the fore

It has become cliché that people are a firms' greatest asset, but people are also the source of greatest risk. The majority of material operational risk events have their roots in either **people doing things they shouldn't** (e.g. rogue traders, people mis-selling retail products, fat finger incidents) or **people not doing things they should** (e.g. people not following policy, people failing to oversee their reports, risk functions failing to provide effective oversight). However, despite its importance, human risk has been neglected by risk professionals and often left to Human Resource departments (often given the pejorative name 'Human Remains') who have tended to focus on administrative support for transactional HR processes and dealing with incidents, rather than supporting proactive human risk management.

However, there are signs in the last year, that Human Risk is attracting much great attention and focus from operational risk professionals (including the popularity of Christian Hunt's Human Risk Podcast and regular newsletters[1]). And indeed, one of the notable aspects of how firms have navigated the Sars-Cov19 lockdowns, has been the attention given to staff welfare and the potential human risks of different working environments. We expect this trend will continue in 2021, with operational risk practitioners focussing on human risk and the application of behavioural science to risk and compliance.

5. Evolving Framework Maturity and use of IT

ORM remains a relatively immature discipline compared to credit and market risk management. However, the discipline continues to evolve, and is becoming noticeably more sophisticated e.g. the increasing focus from the likes of Ariane Chapelle on networks of risks and their interrelationships. In addition, the core tools and concepts are increasingly standardised in line with established good practice, and there are signs that the discipline is achieving a greater balance between regulatory compliance and delivering genuine business value.

We are also seeing more intelligent use of IT systems and 'GRC's (replacing spreadsheets and end-user computing solutions), to support advanced analytics. We are even seeing some use of simple AIs to support identification of subtle linkages and patterns that might otherwise be missed.

With the regulatory focus firmly on operational resilience, we expect this to accelerate the evolution of ORM. We also expect vendor IT systems and GRCs to be a key tool to support firms' efforts to meet regulatory expectations on operational resilience.

Meeting the Future Challenges

Strength comes about by encountering and successfully managing stress, and 2020 has certainly provided stress in abundance!

Making predictions is extremely difficult, especially about the future. But it seems certain there will be more challenges to come, not least from meeting the ongoing challenges of Sars-Cov19, from legal and regulatory change, geopolitical turbulence and from the impact of climate change policies. ORM as a discipline and Operational Risk Managers as practitioners have a key role to play and play it they must. Only then will ORM deliver the outcome of operational resilience, and achieve parity with financial resilience in importance.