Operational Resilience: post-crisis regulation's third act

Stepping into the spotlight

For many in finance, 2018 is remembered for a litany of high-profile outages that dogged the sector. Over the course of a single Spring-Summer, a high-street bank's failed IT upgrade caused it to lose an estimated 10% of its customer base in a week, a payments provider lost its ability to process payments, and an exchange suffered its worst outage in seven years, delaying trade opening for a full hour. Since then, several other outages have famously affected large financial institutions.

> **Operational Resilience:**
> **"An organisation's ability to protect and sustain its core business functions when experiencing operational stress or disruption."**

In all cases, technology failure led to a collapse of the business's core function. A bank is not much of a bank when customers can't access their money and a payments services provider isn't left with much if it can't process payments.

In other words, they were both failures of operational resilience (OR), which PwC has defined as "an organisation's ability to protect and sustain its core business functions when experiencing operational stress or disruption." As a concept, OR doesn't share the same history or recognition of its cousin, financial resilience. However, that's set to change. In July 2018, the Bank of England and the Financial Conduct Authority (FCA) issued a discussion paper entitled "Building the UK financial sector's operational resilience". The paper outlined the supervisory authorities' current thinking on the topic, provided guidance on how to think about it and called for a dialogue on how best to bolster the OR of the financial services sector.

For senior management in financial services firms, it may have seemed as just the latest in an uninterrupted sequence of regulatory focuses du jour. Regulatory fatigue is real and understandable.

However, this represented a broader shift into a third act of post-crisis regulation. Following clampdowns on financial resilience and misconduct risk, operational resilience has emerged as an overarching theme that will continue to guide regulation for years to come.

Underlying this focus is the understanding that firms such as TSB and Visa, who have had issues affecting their customers, are part of an ecosystem of critical financial infrastructure. Without the financial systems that underpin the economy, consumers can't pay for the goods and services they need, businesses can't sell to them and markets can't function efficiently.

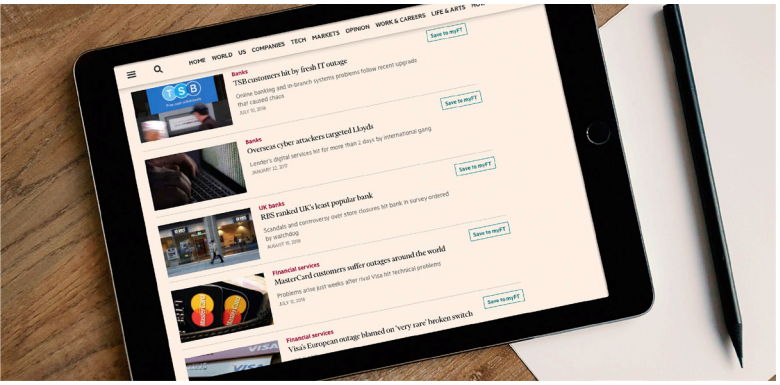
In a digital, always-on world, everything would grind to a halt. The animating principle is the same as that behind financial resilience and capital adequacy rules – these are firms we can't afford to fail. That's why OR has earned its turn to be in the spotlight.

Putting you in the spotlight

What is the price of getting OR wrong? The travails of TSB, Visa and many others serve as effective cautionary tales in many respects. The most obvious risk is financial: TSB faced losses of almost £200m for its failed IT migration, including £115.8m on customer redress. Reputation risk also can't be underestimated: broken trust meant TSB lost nearly 22,000 customers by its own admission.

For senior management in financial services firms, there is another reason to focus on OR: personal accountability.

The discussion paper released by the Bank of England and the FCA in 2018 notes the natural git between a focus on OR and the Prudential Regulation Authority's (PRA) Senior Managers and Certification Regime (SM&CR). Already effective at the time, SM&CR was a response to the 2008 banking crisis, following which the Parliamentary Commission for Banking Standards recommended a new accountability framework for senior management. A key concern was that firms take greater responsibility for ensuring employees were fit and proper and that those employees took personal responsibility for their actions.



Under SM&CR, different functions are assigned to different groups or individuals within a firm based on their role and responsibility. For those categorised as enhanced firms, one such function is the chief operations function (SMF 24). This function is assigned to those who have overall responsibility for the internal operations and technology of a firm, including for OR, cybersecurity and operational continuity.

This will most likely translate to individuals with titles such as Chief Operating Officer (COO), Chief Technology Officer (CTO) or Chief Information Officer (CIO). In some cases, two or more people may share the function with identical levels of seniority.

Whoever ends up designated as the SMF 24 will find themselves with significantly higher personal responsibility. The stakes are raised. If the SMF 24 is found to have made a decision that caused their institution to fail, they are personally open to fines or losing their certificate to work in financial services. From there, knock-on effects to their career stemming from personal reputational damage are quite likely.

In worst case scenarios, they may even be criminally liable. If the SMF 24 was aware, when the decision was taken, that the risk could cause the institution to fail and their conduct fell "significantly below what could reasonably be expected of someone in their position", then prosecution is possible. Seen in this light, OR is less an abstract regulatory concept and more a pertinent personal concern. Not only is OR in the spotlight, but it also puts the spotlight on some of the industry's most senior leaders.

Only the beginning

At the moment, the SMF 24 function only applies to enhanced firms – generally the biggest and most systemically important financial institutions. It is also exclusively a UK regulation.

However, it would be brave to bet on things staying that way. The UK is traditionally a regulatory frontrunner, and decisions made in the UK can generally be read as harbingers for changes to come elsewhere. For example, the European Banking Authority (EBA) is working on a regulatory and supervisory framework aimed at strengthening governance and risk management with a core focus on resilience testing. The G7 countries are also coordinating closely on cyber resilience specifically. In addition to regulatory diktat, it is also likely that firms with broad international footprints that include the UK will apply OR across their organisations.

And, if the breadth of OR's reach is set to grow, so is the depth. Today's financial institutions are unrecognisable in terms of technical complexity from those of just a few years ago. Legacy systems designed for simpler times and needs co-exist with ever increasing layers of interconnected applications and all are expected to coordinate seamlessly with one another. The IT estate only ever grows bigger and more complex.

Consequentially, the goal of OR and the role of the SMF 24 will only become more strenuous over time. The firms best placed to operate confidently and successfully in this environment will be those that invested in effective OR regimes as early as possible – in other words, now. Part two of this series will lay out the steps firms must take to do just that.