King & Spalding

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

SEPTEMBER 8, 2020

For more information, contact:

Robert Dedman
+44 207 551 7552
rdedman@kslaw.com

Kim Roberts
+44 207 551 2133
kroberts@kslaw.com

Penny Froggatt
+44 207 551 7563
pfroggatt@kslaw.com

King & Spalding

London
125 Old Broad Street
London EC2N 1AR
Tel: +44 20 7551 7500

Operational Resilience and the Old Regulatory Two-Step

The UK financial services regulators speak loudly and often about their forward-looking approach to supervision, which – rather than looking back – seeks to focus on future risks to firms and consumers. Yet, you only have to look back at the last financial crisis to know that this exercise can be a bit hit-and-miss. Fast forward to the present day, and the regulators seem – on this occasion at least – to have hit the nail squarely on the head in identifying operational resilience as a key theme for 2020 and beyond.

A SLOW DANCE

Operational resilience has always been a concern for the UK financial services regulators, and there have been rules relating to operational resilience in their handbooks (for example in SYSC 7 and 8) for some time. But, looking back you wouldn't describe the regulatory dance in this arena as a quickstep. It has been more of a slow, leisurely waltz, punctuated the odd flurry from time to time in response to particular incidents.

The classic approach seems to have been for the regulators to respond to an underlying failure of systems and controls that had a significant impact on a firm's systems and, by extension, consumers. For example, in 2014 the Prudential Regulation Authority (**PRA**) and the Financial Conduct Authority (**FCA**) levied a combined penalty of £56 million on the Royal Bank of Scotland group for an IT failure in 2013 that caused significant disruption to the group's banking systems.

The increase in such incidents across the industry has served to bring operational resilience up the regulatory agenda. To put it another way, the tempo has increased, and the music is now playing more loudly.

KEEP YOUR (OUTSOURCE) PARTNER CLOSE

An instructive recent enforcement action arising from an operational resilience failing was the PRA's and FCA's joint action against R Raphael & Sons (**Raphaels**) in July 2019. The Raphaels investigation, which resulted in a financial penalty of nearly £1.9m on the bank, arose out of an IT failure not at the bank itself, but at a sub-contractor which processed payments for prepaid cards issued by the bank. The PRA found that:

- the initial due diligence carried out by the bank on card managers and card processors was inadequate, as were the bank's arrangements for ongoing monitoring;
- the bank's contractual arrangements were poor, and did not include service level agreements covering critical outsourced services; and
- the bank was reliant on card managers to identify and manage the risks posed by failures at card processors.

From a governance perspective, the PRA found:

- the bank's business continuity and disaster recovery planning focused only on the direct actions of the firm, even though the bank relied heavily on outsourced services;
- the bank had no processes for identifying and monitoring the business continuity and disaster recovery arrangements of the outsourced service provider; and
- the bank failed to investigate, and learn lessons from, a previous IT outage at the sub-contractor concerned.

It is also worth noting that, in 2015, the PRA had previously levied a financial penalty on Raphaels for outsourcing failures. While the bank had subsequently undertaken a review of its outsourcing arrangements, the PRA noted that the repeated failure of those arrangements, *"raise[s] serious doubts as to whether that review was adequately scoped, carried out to a satisfactory standard, overseen adequately…and, more generally, of the effectiveness of the [bank's] remediation work…"*

The rather costly impact of this repeated failing was a 40% uplift in the level of the financial penalty levied on the bank.

MOVING INTO THE QUICKSTEP – A JOINT CONSULTATION

The prevalence of cyber incidents and other operational resilience failures arising across the financial services industry (and the pressure brought to bear on the regulators by parliamentary committees) undoubtedly had a hand in bringing this issue to the top of the regulatory agenda, with the result that towards the end of 2019 the PRA and FCA released a joint consultation (building on a discussion paper issued in July 2018) on measures (see the box to the right) designed to lay out more clearly their expectations as regards operational resilience.

Main elements of the joint consultation

The consultation (which is positioned as enhancing rules already in place) included proposals to require firms to:

- identify important business services;
- set appropriate impact tolerances;
- carry out mapping, scenario testing and lessons learned exercises;
- assign a senior manager to be responsible for operational resilience;
- establish a proactive incident communications plan; and
- carry out a self-assessment and provide the FCA/PRA with the results.

COVID-19: THE MUSIC STOPS?

The impact of COVID-19 on the financial sector generally (and on the regulators themselves), led to an announcement that the regulators would extend the time for providing responses to the consultation until October 2020. At time of writing, the consultation is still open.

However, in a classic example of the regulatory two-step, the FCA repeated its expectations that firms take all reasonable steps to meet their regulatory obligations during the pandemic, noting that the consultation paper set out further information on matters that firms should be considering. While this would not make the expectations set out in the consultation paper binding, it was a clear statement of intent from the FCA as to its approach.

TAKING ADVANTAGE OF THE PAUSE

Even though the consultation has been delayed, firms should be under no illusions that the FCA and PRA expect them to be taking steps now to ensure operational resilience in their important business functions. Doing so by reference to the

concepts set out in the consultation paper would seem to be a sensible option, particularly given the content of the FCA's COVID-19 announcement. This could include:

- ensuring that their governance frameworks adequately deal with operational resilience and outsourcing risk;
- ensuring they understand, and take steps to mitigate – including through scenario testing – risks to operational resilience (inside the business and beyond);
- ensuring that an appropriate level of due diligence on operational resilience is carried out into any proposed outsource provider, and any sub-contractor on which the firm's outsourced functions depend;
- ensuring that the contracts with any outsource provider give sufficient rights to obtain information on, and remediate, the provider's operational resilience arrangements and any incident that may affect the firm;
- ensuring that, at all times, they understand the operational resilience systems and controls of any outsourced provider of services, and the potential impact of any incident at an outsource provider;
- consider the impact of COVID-19 on the financial and other resources of outsource providers; and
- maintaining strong arrangements for investigating failures (both internally and by outsource partners);
- ensuring that lessons learned (including from COVID-19) are fed back quickly and effectively into the firm's operational resilience planning process.

The Annex to this document sets out some "Do's and Don'ts" for firms considering operational resilience issues.

Firms supervised by both the PRA and the FCA should remember that – as is so often the case in other areas – the two regulators see operational resilience through quite different lenses. The FCA is focused on the impact on consumers and the markets; while the PRA is looking at the impact on the firm's safety and soundness (and policyholder protection for insurers). This means that when augmenting operational resilience measures (particularly where reporting and MI are concerned) and setting impact tolerances, firms should ensure that both regulators' priorities are catered for.

Finally, given that the COVID-19 pandemic has been - in effect - the first mass test of industry-wide crisis response measures, it is vital that any lessons arising out of the pandemic are fed back into operational resilience planning. At time of writing, the industry is entering a new, and potentially more difficult, phase – where the proportion of staff working from home may fluctuate day by day, week by week. In that context, it will be vital to ensure that systems and controls, particularly those aimed at preventing significant operational incidents such as cyber-attacks, reflect the new more flexible, unpredictable, and fast-paced reality.

LOOKING TO THE FUTURE

When the consultation period closes in October 2020, firms should expect the regulators to firm up their expectations across the industry, with a fairly long implementation period (the consultation paper notes that implementation should take place as soon as reasonably practicable, but not later than 3 years after the rules come into effect). In the meantime, we expect the regulators to be looking carefully at any future operational resilience failures, and potentially opening further enforcement investigations to reinforce the point that this is a regulatory priority.

Given the multitude of threats posed to operational resilience in the financial services industry (from threat actors in the cyber-security space, to changes in working patterns as a result of COVID-19), it seems unlikely that the regulators will move off this patch any time soon. Firms will need to invest significant time and effort in ensuring their operational resilience planning – including in relation to their outsource providers – is sufficiently robust to minimise the likelihood, and impact, of significant incidents right across their business.

DO'S AND DON'TS

✗ **DON'T** assume that issues arising in an outsource provider are irrelevant to the regulated business.

✗ **DON'T** ignore early warning indicators, such as minor failures, which may provide information about the strength of the firm's, or the outsource provider's, operational resilience arrangements.

✗ **DON'T** forget to consider risks arising from the extent to which an outsource provider may sub-contract to other third parties.

✗ **DON'T** forget to review your operational resilience arrangements in response to a significant development, either in the business, the industry or in the wider economy.

✓ **DO** make sure that you map the important functions whose failure would have a significant impact on the firm and/or its customers and take the time to understand the operational dependencies and any associated risks.

✓ **DO** take account of the FCA/PRA consultation paper in dealing with operational resilience matters, as suggested by the FCA in its COVID-19 announcements.

✓ **DO** ensure that any contract with an outsource provider gives you sufficient right to obtain information concerning, and requires rapid remediation of: operational resilience arrangements, and any actual incident.

✓ **DO** ensure that you take account of the different lenses through which the FCA and PRA view operational resilience: consumer protection and market integrity for the FCA; safety and soundness for the PRA.

✓ **DO** consider the impact of COVID-19 on the financial and other resources of outsource providers.

✓ **DO** ensure that the firm considers, and learns any appropriate lessons from, the experience of working during the COVID-19 pandemic.

✓ **DO** make sure that any investigation and remediation work following an incident is appropriately scoped, and resourced.

✓ **DO** ensure that any lessons learned from investigations or reviews are fed back into the operational resilience planning process.

✓ **DO** make sure that the firm reviews its outsource providers', as well as its own, business continuity and disaster recovery arrangements on a regular basis.

✓ **DO** make sure that the firm reviews, on a regular basis, its mapping of important functions and operational risks, particularly when considering new lines of business, or changing outsource providers.

✓ **DO** ensure, when changing outsource providers, that the cut over to the new provider is risk assessed, and appropriately planned and resourced to minimise risk of a failure arising during the transition.

✓ **DO** ensure, if you are a dual regulated firm, that you convey appropriate (and consistent) information concerning any incident to **both** regulators.

✓ **DO** assume, if you are a dual regulated firm, that the FCA and PRA supervision teams will discuss the incident, and the firm's response to it.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	GENEVA	MOSCOW	RIYADH	TOKYO
ATLANTA	CHICAGO	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
AUSTIN	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	
BRUSSELS	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE	