BRIEFING NOTE

OPERATIONAL RESILIENCE

WEATHERING THE NEXT STORM

SEPTEMBER 2020

THINK TANK | COMMUNITY | ADVISORY | TECHNOLOGY | OUTSOURCING

www.crime.financial

THEMIS

INTRODUCTION

There could be no better time to discuss operational resilience than during a global pandemic. As a result of COVID-19, we are currently facing an unprecedented economic challenge that even the best-laid buffers have struggled to withstand, with hundreds of thousands of redundancies announced across the country and an anticipated ticking “corporate insolvency time bomb”.

According to industry research conducted in August 2020, 96% of banking, insurance and healthcare executives feel they have suffered from a lack of business continuity planning in the current environment, with just 16% believing their operations to be “highly resilient” to another crisis. This contrasts sharply with 80% stating confidence in their resilience to cybersecurity threats, demonstrating both the benefit of recent risk focus in this area and the necessity of parity in the preparation for myriad threats.

Lessons currently being learned from the COVID-19 crisis will be helpful for firms’ future operational resilience planning. For example, the pandemic’s effects have highlighted the need for organisations to be more location-flexible and less reliant on paper processes.

DEFINING OPERATIONAL RESILIENCE

Operational resilience refers to the organisational ability to absorb the impact of disruptive events – encompassing IT or telecommunications outages, fraud and financial crime, cyber-attacks, geopolitical incidents, environmental or severe weather disasters, delayed supply and, as mentioned above, pandemics – without exacerbating them.

In practical terms, it relies on an arsenal of techniques and strategies through which staff and processes can flex to continue delivering operations and minimise recovery time. In this vein, business continuity planning represents one aspect of operational resilience.

Rather than focusing on the prevention of disruptive events through risk management – although this is certainly an important exercise for firms – the supervisory authorities define effective operational resilience as the continued provision of services and functions during and after an incident, the limitation of damage done (to customers, the organisation and the market) and the retrospective learning which minimises the chances of a repeat occurrence.

THE REGULATORS' VIEW ON OPERATIONAL RESILIENCE

In December 2019, three consultation discussion papers addressing operational resilience were published by UK regulators. One was authored by the Financial Conduct Authority (FCA), the second by the Bank of England (BoE) and the Prudential Regulation Authority (PRA), and the final one was jointly co-authored by all three regulatory bodies. The discussion papers established the requirement for firms to understand their vulnerabilities and take steps to protect themselves, competitors, consumers and the market from unexpected operational issues – so-called disruptive events. Their publication was largely a response to the Treasury Select Committee's investigation into IT failures within the financial services industry.

While the individual supervisory authorities have long highlighted the need for operational resilience, the very fact of their recent collaboration – the first concerted attempt by regulators to address the issue together – demonstrates its importance for the whole market. Quite simply, the risks associated with the interconnectedness of the financial industry come to the fore in discussions about operational resilience. The supervisory authorities' concern is less with the failure of individual organisations, which they accept is an inevitable part of normally functioning markets, than the subsequent potential for significant disruption to the UK economy.

The discussion paper proposals do not supersede existing requirements set out by these regulators but rather aim to develop new ones that enhance them. Given that the supervisory authorities hold firms accountable for their own operational resilience failures and may fine them accordingly, it is vital that operational resilience is moved up the organisational agenda. It must be reframed from a desirable but optional extra to a fundamental, regulatory requirement.

OPERATIONAL RESILIENCE IN THE FACE OF TECH FAILURES

Pre-COVID-19, the greatest operational resilience threats were conceived of as cyber-based, which is where most firms understandably pooled their efforts. Whilst acknowledging the rise in cyber-attacks and adversaries, and necessity for vigilance in that space, the three aforementioned discussion papers cite the equal potential for disruption from internal threats, such as IT migrations and reliance on tech systems. Indeed, in recent years, a series of high-profile tech issues have served as examples of operational resilience failures, most notably:

TSB

In April 2018, an IT failure left approximately 1.9m TSB customers unable to bank accurately online, following a long-planned IT upgrade to transfer customers from its former parent company, Lloyds, to Sabadell, its new owner. In consequence, TSB lost 80k customers, received 204k complaints, and forfeited £330m in compensation, lost custom, fraud, costs of hiring new complaints staff and retention campaigns. An independent report found that TSB's Board had failed to 'ask the right questions' and adequately assess whether Sabadell's IT arm was capable of carrying out the migration work (it had only run tests on one out of two relevant data centres). The company's Chief Executive resigned but the FCA and PRA's investigations are ongoing. These regulators ultimately have the power to levy an unlimited fine.

Raphaels Bank

On Christmas Eve 2015, 3367 Raphaels customers were left unable to use their bank cards, for which the bank was jointly fined £1.89m by the FCA and PRA for operational resilience failures and weaknesses in management. The specific issues raised by regulators included a lack of adequate consideration of outsourcing by Raphaels' Board, inadequate processes for identifying critical outsourced services, and flaws in the bank's due diligence of providers.

SPECIFIC REQUIREMENTS AND RECOMMENDATIONS ARISING FROM THE DISCUSSION PAPERS

Mapping key business services

An underlying principle of the aforementioned FCA, BoE and PRA discussion papers is the structuring of operational resilience plans according to business services rather than organisational systems - that is, according to the outcome or service expected by the consumer rather than the process by which it is carried out.

This may sound a rather arbitrary distinction but an outcome- rather than process-focused approach should, the supervisory authorities hope, force firms to shift their focus outwards from risk management of internal organisational disruption to mediation of the external effect on consumers and the economy. For example, disruption to one bank's payments may not only prevent its own customers from paying for goods and services but also impair interbank lending, clearing, settlement or mortgage payment, which in turn impacts on other banks, services, businesses and individuals.

The discussion papers ask organisations to identify and prioritise their most important business services as those that, if disrupted, would be most likely to cause "intolerable levels of harm to consumers or market integrity". The regulators expect these services to be classified on a least an annual basis and/or whenever there is a material change to the manner in which an organisation operates (e.g. in the size of its customer base or types of services provided).

To gain a comprehensive understanding of their operational resilience, firms are expected to map – i.e. identify and document the people, processes, technology and resources required to deliver – each of their important business services. Doing so will enable them to pinpoint vulnerabilities and pinch points, such as lack of substitutability, high complexity or dependencies on third-parties.

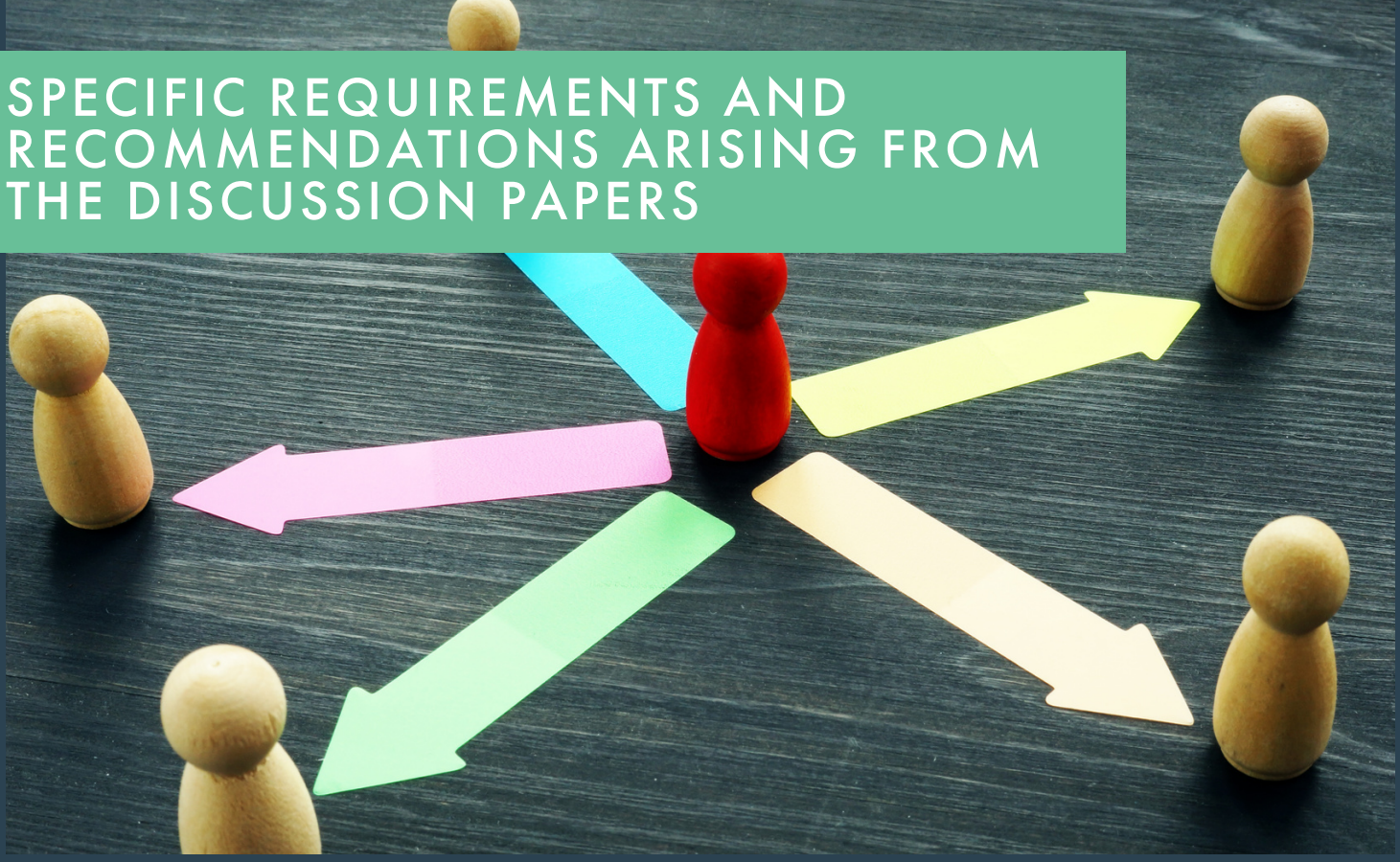
Impact tolerances

Another central tenet of the discussion papers' approach to operational resilience is the concept of impact tolerances. This refers to the "maximum tolerable level of disruption" to an important business service – for example, the "worst case acceptable" duration of a disruptive event on X amount or type of people at which point "intolerable harm" would be felt. The supervisory authorities encourage firms to undertake a more nuanced evaluation of the actual detriment caused to consumers (for example, by prioritising vulnerable customers rather than the largest number).

An example of an impact tolerance in a disruptive event affecting outbound customer payments would be a 25% completion rate within four hours. At least one impact tolerance should be set for every business service defined.

Impact tolerance metrics are subtly distinct from a firm's Recovery Time Objectives, which denote a desirable internal goal rather than a threshold or upper limit of potential harm caused to external stakeholders.

SPECIFIC REQUIREMENTS AND RECOMMENDATIONS ARISING FROM THE DISCUSSION PAPERS



Outsourcing and critical service providers

The supervisory authorities also expect firms to consider operational resilience in relation to outsourcing and third-party services, for which they remain ultimately responsible, especially in the case of critical services like IT and telecommunications. It is worth noting that the supervisory authorities specifically designate Cloud-based data storage providers in their definition of third-party service providers.

According to industry research conducted in August 2020, 60% of organisations were dissatisfied with their outsourcing partners during the COVID-19 crisis, so now is a good time for firms to ensure that their operational resilience work encompasses suppliers and is truly end-to-end, to ensure services can endure through a crisis.

Scenario testing

Firms should undergo a series of specific and “severe but plausible” scenario testing to develop their response plans, with advisable examples including:

- Corruption or deletion of critical data
- Unavailability of facilities, key individuals or third-party services
- Disruption to other firms in the market
- Failure or reduced provision of technology

Scenario testing should factor in whether firms can remain within their impact tolerances and whether doing so compromises market integrity. For example, were firms to resume services to remain within an impact tolerance when they knew there was a significant risk of spreading a computer virus, this would not be considered “tolerable” to the wider market. The discussion papers note that scenario testing should be followed by a “lesson learned” exercise.

SPECIFIC REQUIREMENTS AND RECOMMENDATIONS ARISING FROM THE DISCUSSION PAPERS

Communications

The supervisory authorities highlight the need for documented, meaningful communication processes for internal and external stakeholders during a disruptive event. These processes must cover the gathering of information about the cause, extent and impact of a disruptive event, escalation channels and designated responsibility, and provision of warnings and advice – which should include planning for cases where there is no direct line of communication.

Running throughout the discussion papers, and underpinning firms' approach to operational resilience, is also the importance – and the expectation – of adequate board oversight and access to data for decision-making.

Self-assessment

To document their operational resilience work, the supervisory authorities propose that businesses undergo a self-assessment, verifying all of the aspects described above, i.e.:

Important business services, clearly identifiable as separate services rather than a collection thereof (i.e. withdrawal of cash at an ATM or ability to check an online balance rather than the provision of packaged bank accounts);

- Impact tolerances for the above;
- Approach to mapping (e.g. how they identified resources and vulnerabilities);
- Strategy for scenario testing ability to provide important business services (e.g. a description of scenarios used and any under which they could not remain within their impact tolerances);
- Identification of vulnerabilities and mitigations;
- Lessons learned exercise; and
- Methodologies used to undertake the above activities.

There will be no requirement for this self-assessment to be periodically submitted; rather, it must be available for inspection or sent to the supervisory authorities on request.

HOW CAN THEMIS HELP?

The supervisory authorities already exercise their power to levy fines on companies that display insufficient operational resilience. Ensuring resilience is therefore an essential component of any risk management portfolio. It helps companies to not only avoid financial penalties but also operational losses, compensation to customers and reputational damage in the face and wake of a disruptive event.

The Themis team is experienced in designing and building end-to-end operational risk control and operational resilience frameworks in organisations. Our work is supported with insight we have gained through our valued Themis Community, many of whom have had to address operational resilience challenges themselves.

Our solutions are tailored to suit the specific nature and scale of your operations. We begin with an assessment of your business model and strategy, as well as a gap analysis to identify what you already have in place, adding enhancements if and where necessary. We can analyse your business continuity planning, crisis management documents and REP 18 regulatory reporting requirements, and give you confidence that your organisation meets UK regulatory requirements as well as international standards and best practice (such as ISO 31000 and COSO).

Beyond pandemics, tech reliance and a hostile cyber environment, other global issues such as extreme weather may be more pressing than previously or currently anticipated. Arguably now more than ever, there is an increasing need for strong operational resilience. Coming out of an existing crisis with fresh lessons learned, we must all focus efforts on weathering the next storm.

Please contact one of team to find out more.

Sandeep Sroa
Associate Director
sandeep.sroa@themisservices.co.uk
+44 (0) 7786 236 774

Henry Williams
Head of Investigations
+44 (0) 7780 746 290
henry.williams@themisservices.co.uk

Dickon Johnstone
CEO, Themis
dickon.johnstone@themisservices.co.uk
+44 (0) 7968 537 954