THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

OPERATIONS

Operational resilience

HANNAH McASLAN | ALICE ROUTH
HANNAH MEAKIN | JAMES RUSSELL

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

OPERATIONAL RESILIENCE

HANNAH MCASLAN | Senior Associate, Norton Rose Fulbright LLP
ALICE ROUTH | Associate, Norton Rose Fulbright LLP
HANNAH MEAKIN | Partner, Norton Rose Fulbright LLP
JAMES RUSSELL | Partner, Norton Rose Fulbright LLP

ABSTRACT

Operational resilience has always been a key area of focus for the financial market infrastructure, financial institutions, and their regulators. Traditionally, there was an emphasis on a fairly narrow set of risks and on preventing operational disruptions instead of responding and adapting to them. However, more recently, regulatory focus has shifted as financial institutions have become increasingly vulnerable. Recent papers published by the U.K. regulators are wider in scope, applying to a broader range of financial market participants. Firms are also increasingly expected to place an active emphasis on system resilience in order to enhance the robustness of systems and business processes to futureproof their businesses and reduce the likelihood that an operational risk will occur, but being ready to mitigate the impact when it does, rather than merely reacting to events as and when they happen.

1. INTRODUCTION

Operational resilience is the ability of organizations to continue to deliver critical business services when confronted with adverse operational disruptions by preventing, anticipating, responding, and adapting to such events.

Operational disruption can be caused by a number of internal (e.g., human error or internal technology failures causing system outages) and external factors (e.g., cyber attacks or wider telecommunications failures). The unavailability of critical services can potentially have far-reaching effects. A serious outage can threaten the viability of organizations, cause disruption to customers and other stakeholders, and ultimately jeopardize the stability of the financial system. It can also lead to a reduction in share price, fines from regulators, and in turn, a tarnished reputation. Operational resilience is, therefore, not just about protecting individual organizations, but, perhaps more importantly, it is about protecting the financial system, and those who use it, as a whole. In an environment where firms have increasingly complex operational structures, regulators have had to develop their approach accordingly – they are now taking a broader view of operational resilience to capture all potential risks to critical business services.

Operational resilience is also a source of regulatory risk. Large fines have been imposed on firms that conduct their business in a way that does not meet regulatory expectation in this area. The Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) jointly fined Raphael & Sons plc £1.89m for failing to manage its outsourcing arrangements properly between April 2014 and December 2016. Raphael & Sons failed to have adequate processes to enable it to understand and assess the business continuity and disaster recovery arrangements of its outsourced service providers – particularly how they would support the continued operation of its card programs during a disruptive event. The regulators concluded that the absence of such processes posed a risk to Raphael's operational resilience and exposed its customers to a serious risk of harm.

Firms need to be applying appropriate focus and resources to this area now to be in a position to meet developing regulatory expectations in the future.

2. U.K. REGULATORY FRAMEWORK

Building upon the framework that was outlined in the July 2018 discussion paper, "Building the UK financial sector's operational resilience," produced jointly by the Bank of England, the PRA, and the FCA, the regulators published a suite of documents in December 2019 seeking to further embed operational resilience into the financial system. This included:

- The PRA's consultation paper on outsourcing and third party risk management (CP30/19), which implements the European Banking Authority's (EBA) guidelines on outsourcing arrangements; and
- The PRA's and FCA's consultation papers on operational resilience and impact tolerances for important business services (CP29/19 and CP19/32 respectively).

Operational resilience has also been identified by the FCA in its 2020/21 business plan as one of the five key cross-sector pieces of work.

These proposals set expectations and requirements for firms to identify their important business services and consider the impact that disruption to these services could have beyond their own commercial interests. The regulators have, in this context, identified a number of key themes for firms to consider when assessing their operational resilience. We explore each of these themes in turn below.

2.1 Governance and culture

Regulators expect the culture of a firm to be oriented towards supporting its resilience. All employees need to understand the firm's reliance framework and how they fit into it. In essence, this is about ensuring that a firm can both "survive" and "thrive" – it is not just about a firm's capacity to withstand exceptional strain or points of unprecedented crisis, but perhaps more importantly, how the firm can adapt and manage its way through a crisis or disruption. Further, a firm should be able to anticipate potential stress points in the future so that it can be flexible and evolve with confidence in a dynamic economic, political, and regulatory landscape.

There are a number of key strands to ensuring a culture of operational resilience that have been identified by the regulators:

- **Cultural change to ensure everyone has a clear understanding of operational resilience:** a culture of resilience can be instilled through training, policies and procedures, and company values. Firms need to ensure that an operational resilience culture is embedded in the firm's business model and does not simply coexist alongside the firm's strategy.
- **"Tone from the top":** members of the senior management team need to understand the importance of operational resilience to their firm, and ensure that this message is fed down throughout the organization. Regulators generally expect firms to use their existing governance structures to establish, oversee, and implement an effective approach to operational resilience that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize the impact they have on the delivery of critical operations. Firms should, therefore, be thinking about how operational resilience considerations overlay the frameworks that have been put in place to address (amongst others) requirements flowing from the Senior Management and Certification Regime in the U.K. and other global individual accountability regimes, and ensure that responsibility for operational resilience is assigned to an individual with sufficient seniority and a clear mandate.
- **Operational resilience should drive decision-making and effective challenge needs to be embedded into the firm's organizational structure:** board oversight is required to ensure a holistic application of operational resilience considerations throughout the firm and to avoid management in silos. Key decision-makers at all levels need to receive appropriate management information so that they can exercise their responsibilities appropriately and in an informed way. A culture of challenge should be embedded throughout the organization, from the board and committees down to the way that all individuals perform their roles.
- **Appropriate allocation of responsibility:** alongside the allocation of responsibility for operational resilience amongst members of a firm's senior leadership and the board, firms should ensure that all staff are aware of their responsibilities in this area, and that clear frameworks are in place to map and monitor this allocation. Responsibility for resilience should be assigned across the business, operations, and technology teams and be embedded in the three lines of defense. While the first-line senior management owns and manages risks to resilience, this should be challenged by the second-line. Internal audit also has an important role to play in challenging the governance framework and giving assurance over key resilience capabilities.

2.2 Strategy

Firms need to develop and define a firm-wide operational resilience strategy and operating models that are aligned to the firm's risk appetite.

At the core of this, is the need for the firm to define its impact tolerances and risk appetite framework. This will involve an assessment of the aggregate level and types of risk a firm is willing to assume to achieve its strategic objectives and to ensure the business is run in a way that is aligned to its business plan.

Strategy should be underpinned by a framework that clearly articulates key activities, processes, roles, and responsibilities that enable operational resilience across the firm. Operational resilience should integrate with existing frameworks and set clear expectations for how resilience will be built alongside existing capabilities. In particular, firms should also consider how their "internal capital adequacy assessment process" need to be updated to reflect operational resilience considerations.

Firms should use key performance indicators to monitor the extent to which the business is being run in accordance with the firm's strategic objectives.

2.3 Integration, evaluation, and testing

Each firm needs to consider the way that operational resilience can be built into its business structures. This will involve:

- Mapping the end-to-end service model to understand the systems, processes, people, and third parties that are relevant to the provision of services;
- Identifying important business services that, if disrupted, could cause harm to consumers or market integrity, threaten the viability of firms, or cause instability to the financial system;
- Identifying the metrics that can be used to understand the performance of particular business services and whether issues are being experienced, and creating key performance indicators from this;
- Developing a series of "severe but plausible" scenarios that can be used to stress-test the firm's capacity and capabilities, and in particular, its ability to remain within its impact tolerances. Scenarios should be articulated with a sufficient level of detail to make clear the issue and enable firms to focus on the resulting effects. Disruption scenarios should be tailored to each critical service provided and the impact tolerance and risk appetite for business disruption should be based on the scenarios chosen to be tested. The scenarios can cover issues, such as corruption, deletion or manipulation of critical data, and the unavailability of facilities or key people. Generating these scenarios will require senior engagement. Regulators have historically used simulated incidents to test multiple firms' capacities simultaneously. This can be on a sector-wide basis or to target particular categories of firm;
- Setting impact tolerances for each important business service that quantify the maximum level of disruption they would tolerate;
- Developing a robust testing plan, based on a risk-based approach, to assess the likely impacts of stress tests and stress scenarios across a firm – such plans should be used to assess how the failure of an individual system or process could impact the business service. Stress tests should be well documented, and subject to feedback loops so that the outcome of the test is fed to the right people internally and is appropriately considered. Test results can also be used to identify resilience gaps; and
- Putting in place internal and external communications strategies for when disruption occurs.

2.4 Technology and data

The digital transformation of the economy and increasing reliance on data as a key asset for innovation means that it is crucial that firms place technology resilience at the center of their operational resilience strategy. Cloud computing, artificial intelligence, and innovative IT tools have streamlined the way that many financial institutions operate. Further, a growing reliance on digital technologies and the use of data-driven innovation has led to greater risks of cyber threats.

The COVID-19 pandemic (which is explored below) has further illustrated the increased reliance on digital technologies to enable firms, their staff, and customers to operate remotely and firms have had to digitize at speed. New technologies and new business models bring new risks that must be adequately managed in order to stay within agreed tolerance levels in the event of disruption.

Some of the ways in which firms could look to ensure resilience to ICT-related risks are as follows:

- **Documented ICT policy:** firms are encouraged to ensure that their ICT policy covers cybersecurity with governance and oversight requirements, risk ownership and accountability, as well as business continuity and disaster recovery plans.
- **Incident response and management:** firms should maintain an inventory of incident response and recovery, including any third party resources required to support the firm's response and recovery capabilities. Incident management may include classifying an incident's severity based on pre-defined criteria; developing, maintaining, and testing incident management procedures, including thresholds for triggering business continuity, disaster recovery, and crisis management procedures; implementing communication plans to report incidents to both internal and external stakeholders (such as regulatory authorities) and ensuring compliance with legal obligations in relation to data privacy; conducting an analysis of lessons learned after an incident in order to improve incident response and recovery plans for the future; periodically reviewing incident response and recovery procedures to test and update them where necessary. Any root causes should also be identified and eliminated to prevent recurrence.
- **Identifying critical information assets and infrastructure:** firms should consider their cybersecurity efforts based on the significance of the information assets to their critical operations. They should develop plans in order to maintain integrity of critical information should a cyber event occur.
- **Cyber stress tests:** firms are expected to test for vulnerabilities by conducting cyber stress tests as part of their scenario testing.
- **Regular updates:** technology assets should be kept up to date and patched appropriately in order to help mitigate against cyber threats and risks associated with out-of-support technology.
- **Remote access:** when implementing widescale remote access, as has been required due to the COVID-19 pandemic, firms should ensure that appropriate risk mitigation strategies are in place for disruption or compromise of technology systems and applications. Regular system updates must be rolled out and cybersecurity controls tightened and maintained in order to accommodate remote access as a long-term option.

2.4.1 EUROPEAN APPROACH

On September 24, 2020, the European Commission published its long-awaited proposals on digital operational resilience, comprising a draft regulation, the Digital Operational Resilience Act (DORA), alongside a proposed directive. The package is designed to harmonize and enhance ICT risk management requirements throughout the European financial sector to ensure that all participants of the European financial system can withstand disruptions and threats relating to ICT. The proposals, which are part of the broader Digital Finance Strategy package, aim to harmonize E.U. rules addressing ICT risk and bring major ICT service providers directly within the scope of regulatory oversight. If adopted, DORA would apply to a range of EEA firms, including payment services providers, electronic money institutions, and crypto-asset service providers. DORA covers a number of issues including:

- **ICT risk management:** firms are required to maintain a sound, comprehensive, and well-documented ICT risk management framework, including a dedicated and comprehensive business continuity policy, disaster recovery plans, backup policies, and a communications policy;
- **Incident reporting:** firms are required to establish and implement a specific ICT-related incident management process;
- **Digital operational resilience testing:** firms are required to periodically test their ICT risk management frameworks in a way that is proportionate to a firm's size, business, and risk profile;
- **Managing third party risk and regulating critical ICT service providers:** firms are required to take steps to ensure the sound management of third party ICT risk; and
- **Information sharing:** firms are able to exchange amongst themselves information and intelligence about cyber threats, including indicators of compromise, tactics, techniques, procedures, cybersecurity alerts, and configuration tools.

DORA will not be directly applicable in the U.K., and while there are parallels between DORA and the approach that the FCA and the PRA have set out in their consultation papers on operational resilience, there are important differences that firms will need to consider when developing their implementation strategies. This needs to be worked through thoroughly.

2.5 Customer outcomes

Regulatory attention has been drawn to the way firms react to operational resilience incidents affecting customers (be that end-users or other firms). Consequently, firms should review the mechanisms they use in order to provide real-time updates on a service impacted on their clients. This should include:

- Communicating in a timely, regular, and actionable manner with customers, explaining the firm's response to the crisis incident and the impact this has on the service provided.
- Understanding customer vulnerabilities in line with the impact of operational resilience issues relating to privacy and the use of customer data in remote working environments, and tailoring their handling of different customer groups according to their needs and circumstances.
- Seeking customer feedback and leveraging client-centric metrics in order to plan and respond to evolving customer needs.

2.6 Outsourcing and the use of third parties

Firms are also exposed through their increased reliance on outsourcing arrangements and third party service providers, many of which are not themselves regulated.

Between October 2017 and September 2018, 17% of the incidents that firms reported to the FCA were caused by IT failure at a third party supplier. This was the second highest root cause of disruption to services.

Due to the increasing reliance on outsourcing and third party service providers, firms must have a comprehensive understanding of the resources that support their business services. They must maintain a list of all third parties with whom they do business and who have access to their systems and data. Regulatory developments, including guidelines provided by the European Supervisory Authorities (e.g., the European Banking Authority (EBA) guidelines on outsourcing) have also had a particular focus on operational resilience.

Firms should seek to improve their financial and operational resilience across supply chains, with third parties, and with intra-group entities who deliver critical operations, by considering their dependency on services supplied by third parties and the resilience of third party services.

Firms may look to improve operational resilience across their supply chains and with third parties by:

- **Improving information flows and reporting:** maintaining a comprehensive list of all third parties who have access to their systems and data, including a register of outsourcing (as recommended by the EBA guidelines on outsourcing).
- **Identifying and managing the associated operational risks throughout the lifespan of the third party arrangement:** this should be done from the initial onboarding through business as usual operation and exit or termination of the arrangement. Often, the process of due diligence and onboarding a supply chain partner can be rushed in terms of evaluating their control capacities and it is vital that this must be assessed at the outset in order to provide firms with assurance that risks will be adequately managed.
- **Ensuring that there is not a high level of dependency on a single third party service provider:** where there is dependency on a single provider by multiple firms, this can present challenges if more than one firm wishes to exit an arrangement at the same or at a similar time, or if the service provider suffers a failure that affects multiple firms simultaneously. A high level of concentration within third party service provider arrangements may also reduce or undermine a firm's ability to exert sufficient influence or control.
- **Managing intra-group outsourcing arrangements:** firms should consider the extent to which they are able to exert influence and control over service providers where they are members of the same group or external sub-contractors of intra-group service providers and ensure that effective mitigation strategies are in place.
- **Preventing cross-pollution and risk of a "domino effect" when a supply chain entity faces operational challenges or becomes distressed:** this may be difficult where third party suppliers are operating in multiple jurisdictions with different or lower-quality resilience requirements than those we would expect in the U.K.
- **Establishing an effective and comprehensive procurement process to govern the onboarding of new suppliers:** firms should identify any potential risks arising from the type of service being provided and the way the third party runs its operations, including how it stores and manages data. For example, identifying any issues that have been reported in relation to poor software development practices at the supplier, which have led to security vulnerabilities, will be important in assessing the level of risk when deciding whether or not to contract with that supplier.
- **Developing methods for monitoring the performance and levels of risk associated with third party suppliers:** firms should build open and transparent relationships with their service providers and should regularly monitor their performance. In order to achieve this, firms may wish to define specific roles and responsibilities for each supplier relationship; develop ongoing governance and oversight arrangements, including having periodic meetings; implement and monitor key performance, key risk, and key control indicators in order to assess the performance of each supplier (this may be included in the contractual agreement and will likely include defining what management information is required to be provided and at what intervals); create escalating procedures that allow for issue resolution and feed into the monitoring assessments; and put in place annual control assessments, for example, assurance visits and audits, in order to undertake regular review of performance and outcomes.

2.7 Operations, facilities, and premises

Human error is also a key contributor to operational risk – this can range from a lack of attention to detail to inadequate training.

Firms should leverage their respective functions for the management of operational risk in order to identify external and internal threats. Potential failures in people, processes, and systems should be identified on a regular basis. This will involve:

- A firm's operational risk management function working alongside other relevant functions to manage and address risks that threaten the delivery of critical operations. The firm must coordinate its internal functions, for example, business continuity planning, third party dependency management, and recovery and resolution planning, in order to ensure a consistent approach is taken to operational resilience across the firm.
- Ensuring that sufficient controls and procedures are in place to identify threats and vulnerabilities, and where possible, preventing these threats from affecting critical operations. Where there are any changes to underlying

components of the critical operations, assessments should be conducted in order to ensure that the implemented controls and procedures remain effective.

- Firms should also identify any key facilities and premises that are critical in supporting business services. When carrying out scenario and stress testing, firms should consider the impact of unavailability of facilities or key people in order to develop contingency plans should access to or use of certain premises or facilities become limited. The COVID-19 pandemic has encouraged some firms to realign their approaches to backup locations, as the crisis has demonstrated that teams can effectively work remotely for long periods of time with minimal business disruption.

2.8 Impact of the COVID-19 pandemic

While regulators have seen operational resilience as being fundamental to the way that the markets operate for many years, the COVID-19 pandemic has forced firms to test their operational resilience and has placed particular pressures on the arrangements firms have in place to manage their contingency planning and exposures around operational resilience. There are a number of elements to this:

- **Governance and oversight:** some firms have enhanced their governance and oversight frameworks, including increased frequency of board meetings and the establishment of new response teams. It is important to stress that there is no "one size fits all" approach to governance and oversight as firms' risks will differ depending on their operating model, nature of the services they provide, customer base, and geographical location. As such, firms should assess the situation holistically by creating synergies across their thinking around strategic, financial, and operational resilience.
- **Budget:** firms are reassessing what level of budget they assign to operational resilience. Some firms have been successful in reallocating budget, while for others this presents pressures. The ability to strengthen operational resilience where there are budget constraints will depend to a large extent on the ability firms have to drive down costs and to boost efficiencies.
- **People:** the COVID-19 pandemic has clearly changed how we work, with more people than ever before working from home. The resilience of financial markets and the economy depends on the ability to ensure key workers and the overall workforce can continue to work effectively, whether remotely or from the office. Effective remote working relies on appropriate supervision and oversight, adequate IT software, and broadband connectivity. Firms also need to have arrangements in place for dealing with the scenario where individuals or teams are unable to work for a period of time due to illness.
- **Important business services:** firms have started to map, test, and strengthen their operational resilience frameworks. Identifying key services or critical functions is an important component of this.
- **Outsourcing and systems:** the COVID-19 pandemic has led to some financial institutions retesting the systems that they use to assess the risks associated with third party arrangements in order to ensure that they are able to respond effectively to market pressures.
- **Testing response and recovery capabilities:** most financial institutions test their response and recovery capabilities on an annual basis. However, regulators are urging financial institutions to assess the evolving nature of the operational risks that they face on an ongoing basis so that they can continuously monitor, test, and adapt their recovery plans and capabilities. Further, the ability to learn from the results of the testing response and, importantly, learn how to quickly recover from hypothetical incidents are crucial tools for all financial institutions, enabling them to understand how best to weather the storm and withstand business and operational pressures.
- **Building regulatory relationships:** taking a proactive position with the regulators by creating a regulatory communication plan and being ready to respond to the regulator's requests for information. Firms need to maintain a horizon scanning approach to the rapidly changing regulatory plans and requirements in light of the COVID-19 pandemic.

While firms have been able to respond well to the operational disruption caused by the COVID-19 pandemic, the FCA has stressed that the pandemic has caused a unique style of operational disruption globally. The FCA is encouraging firms to use lessons learned reviews in the wake of the COVID-19 pandemic to test how their systems and processes could be adapted should the next operational disruption take another form (i.e., a cyber attack or technology outage).

3. CONCLUSIONS AND NEXT STEPS

It is expected that the FCA and the PRA will look to finalize their approach to operational resilience in 2021, with firms needing to implement necessary changes by 2022. Firms are encouraged to not wait until the rules are finalized to formulate their approach, but instead they should be placing a greater focus on operational resilience now. Many firms are using the experience of the COVID-19 pandemic as a catalyst for this exercise since it has in many respects required them to make a start.

Firms looking to assess their operational resilience should start by asking themselves the following questions:

1. What are the firm's important business services?
2. Has the firm set impact tolerances for each important business service?
3. Has the firm tested its ability to remain within its impact tolerances through a range of severe but plausible disruption scenarios?
4. Has the firm identified the resources that support its important business services?
5. Does the firm have a clear communication plan for when business services are disrupted?
6. Would the firm be able to effectively demonstrate how it will meet operational resilience requirements?

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO