BUILDING OPERATIONAL RESILIENCE

SUMMARY

Shortly before the holiday season in December 2019, the FCA, PRA, and the Bank of England published a joint policy summary as well as separate consultation papers on operational resilience (including changes to the FCA Handbook and PRA Rules and new PRA Supervisory Statement). The proposals contain a new regulatory framework for operational resilience, requiring regulated firms to develop systems, processes and operations to ensure their ability to provide important business services in times of operational disruption. These proposals will require firms to mobilise resources and launch "top-of-the-house" implementation projects to meet new standards of operational resilience. Failure to implement would risk regulatory enforcement against the firm and senior managers.

The increased regulatory focus on operational resilience stems from a combination of factors, including: a shift in the way customers access financial services by using digital services; the use of new technologies to improve services; the significant negative impact of IT failures/incidents, with major incidents at RBS, TSB and Visa; and the introduction of new types of risk such as cyber security risk. Increased reliance on outsourcing, with its use of technological innovations and new methods of delivering business operations, has also further rendered firms vulnerable to disruption risk.

Key issues

THE PARAMETERS OF OPERATIONAL RESILIENCE – KEY DEFINITIONS

One practical consideration is how the proposed framework on operational resilience sits alongside existing programs that firms have put into place in order to comply with other regulatory requirement such as operational continuity in resolution (OCIR), business continuity planning, operational risk, and outsourcing regulatory requirements.

The UK regulators define operational resilience as the ability of firms to provide important business services in times of operational disruption and have proposed an outcomes-based approach for the regime. Whilst firms should continue to take steps to avoid disruption, operational resilience ultimately focuses on recovery, learning and improving and is the overarching framework under which the existing regimes sit.

For example, OCIR aims to ensure continuity of critical functions from an operational perspective through severe stress and resolution. It is closely linked to operational resilience but has a narrower scope since operational resilience covers continuity in all disruptions. Likewise, both operational risk and outsourcing can be considered as sub-sets of operational resilience, given that they have a narrower scope of focus - they are not sufficient, in

themselves, to ensure continuity of business services. Specifically, while operational risk measures the severity of the impact of disruption, the focus assumes that the risk has not yet crystallised and this measurement is merely a part of the requirement of firms to manage risks prudentially and, if necessary, hold capital buffers. Outsourcing raises continuity issues as it involves the delivery of a business service or activity by another entity but as firms need to be operationally resilient regardless of any outsourcing arrangement, the outsourcing regulatory framework supports wider operation resilience.

The key issue for firms is bringing together different programs, teams and silos which aim to comply with existing requirements and refocus their energies under the new operational resilience umbrella from the perspective of important business services.

BUILDING OPERATIONAL RESILIENCE

The proposed regime requires firms to assume that a disruption has crystallised and to respond to, and recover from, an incident. Disruption risks are contingent upon the nature of the institution, and banks, for instance, may face qualitatively and quantitatively different risks from those faced by asset managers. However, in practical terms, all firms should assume disruption events will happen quickly and therefore that careful forward preparation is essential. Given the global, automated and technology-based nature of the financial services industry, these events can rapidly affect a large number of transactions and individuals.

In building operational resilience, firms must identify important business services and comprehensively map the people, processes, technology and information that support these important business services. In addition, firms will be required to:

- set **impact tolerances** (thresholds for maximum tolerable disruption) for each important business service (two impact tolerances for dual-regulated firms);
- **test** the firm's ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios, including corruption, deletion or manipulation of critical data and the unavailability of facilities or key people;
- conduct **lessons learned exercises** to identify, prioritise, and invest in the firm's ability to respond and recover from disruptions as effectively as possible;
- developing internal and external **communications plans** for when disruption occurs; and
- create a **self-assessment** document detailing all steps taken to ensure operational resilience.

IDENTIFYING IMPORTANT BUSINESS SERVICES

The first key challenge for firms in the implementation of the proposed regime will be to identify important business services.

A business service is one which a firm provides to an external end user or participant and an important business service is a service that, if disrupted, would be likely to cause intolerable levels of harm to consumers market

integrity or safety and soundness of financial stability. UK regulators propose that firms should identify their important business services at least once a year and following any material change to their business.

Given that the importance of services depends on the nature of the institution, regulators do not plan to introduce definitive taxonomies of important business services, but have rather taken the view that firms are best placed to identify their own important business services. The key characteristics are that the business service should be a separate service distinguishable from a line of business and that users of the service should be identifiable.

In practice, UK regulators have suggested a non-exhaustive list of indicative factors that firms should have regard to when considering whether disruption to a service would cause intolerable harm, focussing on the likely impact of the disruption on the consumer base, the firm itself and the UK financial system, as well as the likelihood of the disruption threatening the safety and soundness of the firm and financial stability.

SETTING IMPACT TOLERANCES

The second key challenge for firms is to set impact tolerances that quantify the maximum amount of disruption that a firm could tolerate in a disruption incident. Impact tolerances are viewed by regulators as an efficient tool for boards and senior management to set standards for operational resilience and therefore prioritise resources and investment decisions.

Impact tolerances are expressed by references to a specific outcome and metrics which must include the maximum acceptable outage time for an important business service. When setting impact tolerances, firms must take into account factors which indicate harm, for instance, number and type of customers or market participants who are adversely affected by the disruption or financial loss to customers or market participants.

Firms need to test their ability to stay within impact tolerances in severe but plausible scenarios which may include the occurrence of multiple disruption events at the same time. Impact tolerances set the upper limit as to when important business services will continue in certain scenarios but there will be extreme scenarios in which firms will not be able to continue the provision of an important business service. This testing reveals vulnerabilities in systems and processes and what mitigating actions need to be taken for the firm to stay within the impact tolerances.

Firms must be able to remain within their impact tolerances as soon as reasonably practicable, but no later than three years from the date that the regime comes into force.

CUSTOMER IMPACT

During and after a disruption event, firms must ensure that they consider the impact on customers who could be affected. The FCA has placed particular emphasis on the continuity of business services to which customers have access rather than specific products. For example, in a retail context, such disruption events affecting customer-facing business services could mean that accounts become inaccessible or funds transfers no longer possible. Similarly, in an asset management context, investments may be left unmanaged or investors may not be able to liquidate their assets in a timely manner resulting in adverse knock-on consequences. As such, proper customer care should entail, at least, customer communication from the outset

of the event, putting in place measures to assist customers while the disruption is resolved, and liaising with customers post-disruption to fully understand the impact of the disruption.

GOVERNANCE AND SENIOR MANAGEMENT ACCOUNTABILITY

UK regulators are looking to hold senior managers to account with respect to operational failures. This is also brought sharply into focus given that the Senior Managers Regime applies to all firms from 9 December 2019. In this respect, the FCA has expressly identified the role of Chief Operations Function (SMF 24), which generally covers internal operations, as also covering operational resilience, cybersecurity and operational continuity.

Firms are encouraged to ensure that senior managers have appropriate awareness of the operational risks which could affect the firm, to allocate clear senior management responsibility and accountability for operational resilience, and to allocate senior management representation in overseeing a firm's response to a disruption event when one does occur. Moreover, firms should ensure that senior managers surround themselves with clear and clean governance and that they have a "three lines of defence" approach.

The board will also be responsible for exercising oversight over the management's delivery of operational resilience. Firms will be required to produce appropriate management information for the board in order to properly perform its oversight role. In addition, the board will need to review and approve regularly the firm's self-assessment of its operational resilience.

IBOR TRANSITION

One of the most significant upcoming risks to which firms will have to demonstrate resilience will be the large-scale change programmes necessary to effect the phase out and replacement of IBOR by the end of 2021.

This complex transition brings with it a considerable risk of disruption: most firms will have to consider reconfiguring primary trading systems, updating data sourcing systems, reviewing risk management and valuation tools and adapting asset and liability management systems. Firms will therefore need to demonstrate their operational resilience to the potential disruptions arising from the transition. This will include securing appropriate staff expertise, updating technological infrastructure and testing new platforms. It will also involve retaining project teams following rollout to provide ongoing support, ensuring suitable backup systems are available as necessary and clearly designating senior management accountability for transition oversight.

Given the timing of the recent consultation papers, regulators will be closely scrutinising the preparations made by firms to effect IBOR transition, and will expect the guidance set out in the papers to be diligently followed. Given the transition's significant scope for disruption, the considerations in the context of the change illustrate how important it is for a firm to be continually cognisant of its operational resilience.

ENFORCEMENT ACTIONS

Unsurprisingly, increased regulatory scrutiny on firms' operational resilience has resulted in an increase in enforcement action. Recent examples include the FCA's enforcement decision relating to Tesco Bank in November 2018, following the firm's response to a cyber-attack, and the FCA and PRA's

enforcement decisions relating to Raphaels Bank in April 2019, following an IT outage at the firm's outsourced card processor.

Enforcement action is not restricted to financial regulators given the broad nature of operational resilience. The ICO has fined numerous firms for compromising the personal data of customers as a result of failures to ensure proper safeguards against cyber-attacks. Most recently, DSG Retail was fined the maximum statutory amount by the ICO in January 2020, for allowing the personal data of 14 million customers to be hacked as a result of poor cyber security.

In addition, overseas regulators are increasingly bringing enforcement actions against institutions relating to operational resilience failings. For example, the Central Bank of Ireland has recently issued a penalty as a result of an institution failing to have adequate control systems to ensure that it satisfied outsourcing requirements.

With respect to enforcement against individuals, the FCA and PRA were asked by the Treasury Select Committee in June 2019 about the personal accountability of senior managers in the specific context of IT failures. The regulators stated that senior managers were the subjects of several ongoing enforcement actions for their role in firms' poor operational resilience. The Treasury Select Committee was emphatic that regulators must use all enforcement tools at their disposal to hold individuals to account in this respect.

The issues arising from these enforcement actions have been reflected to a large extent in the recent consultation papers. The decisions illustrate a marked shift in regulatory expectations on firms in the context of disaster recovery, from a reactive "fix on fail" approach to a much more proactive assessment of a firm's resilience. The codification of increased expectations on firms in the consultation papers suggest that enforcement action is only likely to increase.

CONTACTS

Monica Sah
Partner

T ++44 207006 1103
E monica.sah
@cliffordchance.com

Kate Scott
Partner

T +44 207006 4442
E kate.scott
@cliffordchance.com

Nicholas Grafton-Green
Senior Associate

T +44 207006 8439
E nicholas.graftongreen
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ