protiviti®
Face the Future with Confidence

U.K. Supervisory Authorities and Basel Committee Refine Operational Resilience Approaches, Align on Expectations for Firms

Several Key Policies Take Effect March 31, 2022

On March 29, 2021, the Bank of England (BoE), the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) issued a series of policy statements to both refine and finalise their approach to operational resilience for financial services firms. Almost concurrent with the release of the policy statements, the Basel Committee on Banking Supervision (BCBS) issued its principles for operational resilience.

The U.K. regulatory authorities' policy statements, which follow a July 2018 discussion paper and a December 2019 string of consultation papers, are contained in these documents:

- Overall supervisory approach
- PRA statement
- FCA statement
- PRA statement on outsourcing and third-party risk management
- BoE's approach for financial market infrastructures (FMIs)

The well-timed BCBS principles document is a refinement of its resilience expectations for banks, but, like those of the U.K. supervisory authorities, does not represent a significant deviation from its earlier views on the topic. The document, Principles for Operational Resilience, builds on BCBS' Principles for the Sound Management of Operational Risk, and draws from its previously issued principles on corporate governance for banks, outsourcing, business continuity and relevant risk management-related guidance.

Together, the BCBS principles and the U.K. supervisory authorities' policy statements represent the most detailed regulatory thinking to date on the topic of resilience, providing

organisations a potpourri of principles and rules-based approaches to address their resilience needs.

A Pragmatic Approach with Clear Timelines

In the policy statements, the U.K. supervisory authorities clarify their operational resilience expectations for U.K. financial services firms, scarcely straying from previous positions. In addition to affirming their preference for a pragmatic regulatory and compliance approach, they outline specific operational resilience requirements and timelines for implementing certain policy requirements.

Overall, the policies are not as prescriptive as some firms may like (particularly as they relate to testing and self-assessment). The supervisory authorities want firms to have the ability to apply flexible and proportionate methods to enhancing their resilience, but also intend to take an outcomes-based approach, as they continue to monitor how institutions manage and implement resilience.

Regarding their expectations of when firms are to address various policies, the supervisory authorities established the following key timelines:

- Identify important business services and set impact tolerances: **March 2022.**
- Perform mapping and scenario testing to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities in their operational resilience: **March 2022.**
- Create a strategy and/or plan for compliance: **March 2022.**
- Manage resilience as business as usual and remain consistently within impact tolerances: **March 2025.**

Below is a summary of key policies and principles that are clarified in the latest documents:

Important Business Services or Processes

The U.K. supervisory authorities' policy statements make it clear that firms are to identify only their important business services — not all services — for the purposes of operational resilience. Regarding what qualifies as "important business services," the authorities ring-fenced their focus on the services most critical to external end users, customers or market participants, and what is required to deliver those services. In the final policy, so as to avoid expanding the coverage of the policy and to ensure that the focus remains on the most important external services, the authorities opted to not include internal processes (such as

payroll or human resources) in the definition of important business services. They recommend that internal processes essential to the provision of important business services be captured by mapping to facilitate any remediation work that firms may be required to perform after a disruption.

Meanwhile, in the principles document, the BCBS uses the term "critical operations" in lieu of "important business services." The term is based on the Joint Forum's 2006 high-level principles for business continuity, and encompasses "critical functions," a commensurate term for important processes as defined in the FSB's 2013 recovery and resolution planning guidance for systemically important financial institutions. Notwithstanding the variation in terminology, both the U.K. authorities and the BCBS appear to be focused on understanding firms' operations, their role in the financial systems and dependencies on specific businesses that could cause harm to various stakeholders in the event of a disruption.

Impact Tolerance

Of the operational resilience concepts, impact tolerance has so far generated the most vigorous debate. The new policy statements do little to quell the contentious points. How to calculate impact tolerance and what methodology to use are still firm-dependent, with the regulators appearing to defer any possible regulation toward a particular method until they learn the outcome of industry exercises. Nonetheless, the supervisory authorities state explicitly that a time component should be included in the calculation of impact tolerance, a necessary conclusion affirmed in the December 2019 consultation papers.

Additional guidance is provided on what constitutes intolerable harm, defined as harm from which consumers cannot easily recover. An example of this could be a firm that is unable to put a client back into a correct financial position post disruption or where there have been serious nonfinancial impacts to customers (e.g., loss of functionality or access or loss of confidentiality, integrity or availability of data) that cannot be remediated effectively.

In the FCA statement, there is a notable focus on consumer vulnerability. This has been a key area of interest in the FCA's annual plans over the past few years and has been at the top of the regulatory agenda with firms and even more so since onset of the COVID-19 pandemic. Given this escalated focus, firms should work closely with their conduct risk teams or equivalent to appropriately consider consumer vulnerability when setting impact tolerances.

While impact tolerance will need to be thought through and set to meet both the FCA's and the PRA's objectives, in practice, assessing the firm's ability to meet them will be largely focused on maintaining the lower of the two. The PRA has also narrowed the scope of its

rules so that smaller firms will not need to consider financial stability when setting impact tolerances.

While the BCBS does not explicitly call out impact tolerance, it alludes to the concept with the term "tolerance for disruptions," which it defines as "the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios." In considering their operational resilience, the BCBS states that banks should take overall risk appetite and tolerance for disruption into account, essentially aligning with the U.K. regulators that firms need to understand the level of downtime they are willing to accept.

Mapping

The supervisory authorities reemphasise the need for firms to map important business services and provide guidance on performing those activities. According to the policy, mapping should be sufficiently detailed to allow firms to understand the resources (i.e., people, processes, technology, facilities and information) necessary to deliver important business services, irrespective of whether they use third parties in the delivery of these services. To help firms understand exactly what to map, the policy statements define the people, processes, technology, facilities and information that support the operation of an important business service.

In the BCBS principles, banks, once they have identified their critical operations, are encouraged to "map (i.e., identify and document) the people, technology, processes, information, facilities, and the interconnections and interdependencies." It is no surprise that there is clear alignment between this principle and the goals of the supervisory authorities, as mapping is a linchpin to understanding the resilience of a firm's operations.

Scenario Testing

Testing has been a keen focus of the supervisory authorities since the initial discussion paper was issued by the U.K. supervisory authorities in 2018, with emphasis placed on a firm's ability to test, understand and act on lessons learned, and to consider severe but plausible (or extreme but plausible, in the case of FMIs) scenarios. Similar to mapping, firms are now expected to perform scenario testing to a level of sophistication necessary to identify accurately their important business services, set impact tolerances and identify any vulnerabilities in their operational resilience.

The new policy does not require testing to be undertaken at least every year as previously prosed. Rather, regular scenario testing is required when there is a material change to the

business, infrastructure or impact tolerance, or following improvements made in response to a previous test. The time and effort involved in regular testing will no doubt create additional costs. Firms may participate in industrywide testing, which may be developed over the longer term as part of a wider supervisory approach.

The importance placed on testing by the supervisory authorities in testing is also conveyed in the BCBS principles, which not only reference the need for testing but also call out business continuity planning and incident management, two of the seven principles in the document.

Self-Assessment

No templates were provided for self-assessment. Rather, the policy statements encourage firms to share best practices via working groups, and stipulate that the earliest date a self-assessment would be formally requested is March 31, 2022. The BCBS principles do not address self-assessment.

What's Next

The tranche of policy, supervisory and principles-based statements affirms the growing regulatory importance of operational resilience. By crystallising certain prior proposals into policy and issuing timelines around the implementation of key requirements, global standard setters and the U.K. supervisory authorities have officially put firms on notice to act now to prepare for formal operational resilience regulation. With respect to the timelines for compliance issued by the supervisory authorities, a year is not a significant amount of time for firms — particularly larger financial institutions that may need to stand up or refine their approach to resilience before the rules kick in.

Now is the time for firms to allocate the necessary resources to address what is becoming not just a U.K. mandate, but a global one as well. This begins with firms' understanding the clear outcomes and expectations for building operational resilience as outlined by the supervisory authorities, and how success will be measured based on minimising harm to customers and the number and types of operational disruptions they are able to prevent, respond to, and recover and learn from.

How We Help Companies Succeed

Protiviti's financial services industry experts help organisations demonstrate and improve resilience through a robust testing program, building on existing business continuity management activities, IT disaster recovery and cybersecurity incident response. We work with and report to executive leaders and the board to address such questions as:

- Have we formally defined the important functions and services vital to the execution of the business model?
- Are impact tolerances established and tested?
- Are front-to-back mappings of components of the important functions and services understood and maintained?
- Is there a structure in place to govern resilience across the enterprise properly?
- Are severe but plausible scenarios tested regularly?

Additionally, we partner with organisations to develop their overall operational resilience internal audit plans, incorporate operational resilience into existing audits and provide assurance over the operational resilience program. Click here to access Protiviti's operational resilience framework and additional thought leadership on the topic.

Contacts

Carol Beaumier
Senior Managing Director,
Risk & Compliance
+1.212.603.8337
carol.beaumier@protiviti.com

Ron Lefferts
Managing Director,
Global Leader of Technology Consulting
+1.212.603.8317
ron.lefferts@protiviti.com

Michael Brauneis
Managing Director,
North America Financial Services
Industry Leader
+1.312.476.6327
michael.brauneis@protiviti.com

Matthew Moore
Managing Director,
Global Risk & Compliance Leader
+1.704.972.9615
matthew.moore@protiviti.com

Douglas Wilbert
Managing Director,
U.S. Operational Resilience Leader,
Risk & Compliance
+1.212.708.6399
douglas.wilbert@protiviti.com

Bernadine Reese
Managing Director,
U.K. Operational Resilience Leader,
Risk & Compliance
+44.207.024.7589
bernadine.reese@protiviti.co.uk

Thomas Lemon
Managing Director,
U.K. Operational Resilience Leader,
Technology Consulting
+44.207.024.7526
thomas.lemon@protiviti.co.uk

Laura Moore
Director,
Risk & Compliance
+44.207.024.7591
laura.moore@protiviti.co.uk