protiviti®
Face the Future with Confidence

# Early Signs of Regulatory Alignment on Operational Resilience Concepts, Themes

In early August 2020, the Basel Committee on Banking Supervision (BCBS) released a consultative document, titled "Principles for Operational Resilience," that proposed a pragmatic yet flexible approach to operational resilience, one intended to be principles-based. Publication of the consultative document was expected and timely, coming amid a growing regulatory focus on operational risks and the COVID-19 pandemic.

The principles outlined by the BCBS align with the overall view of operational resilience in the discussion papers published by the UK supervisory authorities, namely the Bank of England, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), in December 2019, although those papers present a much more prescriptive approach. This alignment among the regulatory bodies is further affirmation for many firms that have been developing or realigning their resilience programs since the summer of 2018, when the UK supervisory authorities introduced its first discussion paper on operational resilience.

While it is similar in tone and substance to the other papers, there are some slight differences in the terms and themes used in the BCBS consultative document, a variance that may be attributed to the BCBS building on its previous papers to align to its own definitions. Nevertheless, the divergence is minimal and probably intended, as the BCBS typically strives to design potential policy measures that appeal to a wide array of stakeholders, including membership from 28 jurisdictions worldwide.

The following are two minimal differences in the BCBS' document:

- Whereas the UK supervisory authorities note the importance of business continuity and cybersecurity, the specific callout by the BCBS on business continuity planning and testing, as well as information and communications technology (ICT) cyber security, is more pronounced. Our belief is that COVID-19 concerns compelled the BCBS to highlight these present-day concerns.

- The BCBS paper does not provide a definition for "impact tolerance" – the term that pertains to a point in time when the viability of an important business service is irrevocably threatened – or a corresponding metric. Rather, the paper calls for feedback on useful metrics for resilience, adding that "operational resilience is in a nascent stage and further work is required to develop a reliable set of metrics that both banks and supervisors can use to assess whether resilience expectations are being met."

The concept of impact tolerance has been heavily discussed since 2018, with industry leaders and regulators considering various definitions and approaches. The UK supervisory authorities have offered some flexibility in determining impact tolerances, although they have made it clear time is an essential element. Specifically, they propose that, where relevant, institutions may decide also to include other metrics, such as volumes and values, in their impact tolerances, given that a metric based on time alone may be insufficient.

The BCBS emphasizes the role of governance in achieving operational resilience. In line with other published regulatory views that setting the right "tone from the top" is essential for building resilience, the BCBS proposes that boards should be held responsible for reviewing and approving banks' operational resilience expectations, considering each organization's risk appetite, risk capacity and risk profile. The BCBS' view on governance is in lockstep with our own experience; we have consistently found that the success of a resilience program is highly correlated to senior management buy-in and active engagement.

As the industry weighs various approaches and proposals to building resilience, an exercise that has become more urgent considering the COVID-19 pandemic, we expect operational resilience taxonomy to continue to evolve. The BCBS, which is inviting comments on its proposals through the end of the consultation period on November 6, 2020, has indicated it will monitor the impact of the pandemic and any lessons learned to help inform its final guidance on operational resilience. While we cannot anticipate the outcome of the pandemic and its influence on future guidance, we do not expect the pandemic's impact to alter the principles proposed by the BCBS.

Meanwhile, the Federal Reserve Board, which lists operational resilience of critical systems among its 2020 supervisory priorities for large institution, is expected to weigh in on the topic by the end of the year. The Fed, through a senior official, previously signaled it is open to a rules-based approach that incorporates leading industry standards and best practices.

The UK supervisory authorities extended their consultation period from early April to October 1, 2020 to give firms more time to address COVID-19 concerns. The EU Commission is also expected to have papers forthcoming this year on the topic. We do not anticipate a similar release from the U.S. Office of the Comptroller of the Currency (OCC), although operational resilience is among the priorities in its 2020 supervision plan.

## What's Next

Based on the present public guidance and our analysis, we believe the UK supervisory authorities will continue to be the more prescriptive regulators on this topic, and the Fed and

the EU aligning with the BCBS in tone and detail. And, while there is certainly agreement on the topic, it will be interesting to see if there are any nuanced differences in how firms are regulated under resilience.

For now, we have compiled a list of key terms and definitions around resilience (**Table 1**) that have so far been proposed by various regulatory bodies. This is not an exhaustive list of all regulatory proposals on operational resilience, but rather a compilation of the more developed views on this evolving topic. Some are aligned and others are not, but the intent is clear: Resilience is top of mind and not going away.

In **Table 2**, several high level BCBS principles are compared to relevant excerpts from the UK supervisory authorities' papers on operational reliance. The themes discussed are consistent with those in the documents.

## Table 1

| Term | Basel Committee on Banking Supervision[1] | UK Supervisory Authorities[2] | International Organization of Securities Commissions (IOSCO)[3] | Monetary Authority of Singapore Consultation Paper[4] |
|---|---|---|---|---|
| **Operational Resilience** | **Term used:** Operational Resilience<br><br>**Definition:** The ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events to minimize their impact on the delivery of critical operations through disruption. | **Term used:** Operational Resilience<br><br>**Definition:** The ability of firms and financial market infrastructures (FMI) and the financial sector as a whole to *prevent, adapt, respond to, recover* and *learn from* operational disruptions. | **Term Used:** N/A<br><br>**Definition:** N/A | **Terms used:** Resilience, Operational Resilience<br><br>**Definition:** Not defined |

[1] *Principles for Operational Resilience*, Basel Committee on Banking Supervision: www.bis.org/bcbs/publ/d509.htm.

[2] *Building the U.K. Financial Sector's Operational Resilience*, Bank of England: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

[3] *Principles for Financial Market Infrastructures: Disclosure Framework and Assessment Methodology*, IOSCO, December 2012: www.iosco.org/library/pubdocs/pdf/IOSCOPD396.pdf.

[4] *Proposed Revisions to Guidelines on Business Continuity Management*, Monetary Authority of Singapore, March 2019: https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-Paper-on-Proposed-Revisions-to-Business-Continuity-Management-Guidelines.pdf.

| Term | Basel Committee on Banking Supervision[1] | UK Supervisory Authorities[2] | International Organization of Securities Commissions (IOSCO)[3] | Monetary Authority of Singapore Consultation Paper [4] |
|---|---|---|---|---|
| **Important Business Services** | **Term Used:** Critical Operations/Critical Functions<br><br>**Definition: A**ctivities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external and internal interconnectedness, complexity and cross-border activities. Examples include payments, custody, certain lending and deposit-taking activities in the commercial or retail sector, clearing and settling, limited segments of wholesale markets, market making in certain securities and highly concentrated specialist lending sectors. | **Term used:** Important Business Services<br><br>**Definition:** A service provided by a firm or FMI to an external end user or participant where a disruption to the provision of the service could cause intolerable harm to consumers or market participants; harm market integrity; threaten policyholder protection; safety and soundness; or financial stability. | **Terms used:** Critical Operations and Services<br><br>**Definition:** Not Defined | **Term used:** Critical Business Function<br><br>**Definition:** A business function, which, if disrupted, is likely to have a significant impact on a financial institution, whether financially or non-financially. |
| **Impact Tolerance** | **Term Used: N/A** | **Term used:** Impact Tolerance<br><br>**Definition:** The maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption. | **Terms used:** N/A<br><br>**Definition:** N/A | **Term used:** Minimum Performance Level<br><br>**Definition:** Not defined |

## Table 2

| Theme | BCBS Principle | UK Supervisory Authorities |
|---|---|---|
| **Governance** | Banks should utilize their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their impact on delivering critical operations through disruption.<br><br>The board of directors should review and approve the bank's operational resilience expectations considering the bank's risk appetite, risk capacity and risk profile. In formulating the bank's risk tolerance for disruption to its critical operations, the board of directors should consider a broad range of severe but plausible scenarios (e.g., lockdown due to pandemics, destructive cyber security incidents, catastrophic natural disasters, etc.). | Management bodies would need to have sufficient knowledge, skills and experience to meet their operational resilience responsibilities. This should ensure the management body can challenge senior management constructively on the firm's or FMI's operational resilience and the management body can meet its oversight responsibilities.<br><br>**PRA**:<br>Boards are specifically required to approve the important business services identified for their firm and the impact tolerances that have been set for each of these. The operational resilience parts require that a firm's board must approve and regularly review the firm's important business services, impact tolerances and written self-assessment. In delivering this responsibility, boards must regularly review assessments of the firm's important business services, impact tolerances, and the scenario analyses of its ability to remain within the impact tolerance for these important business services. |
| **Operational Risk Management** | Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience expectations. | Risk appetites focus management attention on managing the likelihood of operational risks occurring, and the impact if they do. The introduction of impact tolerances will increase the focus of firms and FMIs on their operational resilience before operational risks have crystallized. This should increase their capability to survive severe (or in the case of FMIs, extreme) disruptions when risk appetites are likely to have been exceeded. Impact tolerances are also set only in relation to harm to consumers or market participants, harm to market integrity, or threats to policyholder protection, safety and soundness, and the wider financial sector. |

| Theme | BCBS Principle | UK Supervisory Authorities |
|---|---|---|
| **Business Continuity Planning and Testing** | Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption. | The UK supervisory authorities stated that, in addition to developing policy proposals, they would be drawing together existing policy material, which is relevant for the operational resilience of firms and FMIs. When considering other policies such as operational risk and business continuity planning, firms and FMIs should consider how the application of these policies support the delivery of important business services. |
| **Mapping Interconnections and Interdependencies** | Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations. | A firm or FMI must identify and document the necessary people, processes, technology, facilities and information (referred to as resources) required to deliver each of its important business services.<br><br>The supervisory authorities do not propose to be prescriptive on a mapping process. Firms and FMIs can develop their own methodology and assumptions to best fit their business. Firms and FMIs could use methods such as process mapping, transaction life cycle documentation, and customer journeys. |
| **Third-Party Dependency Management** | Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations. | Firms should ensure that their important business services are able remain within their impact tolerances even when they rely on outsourcing or third-party providers.<br><br>* Bank of England consultation paper: *CP30/19: Outsourcing and Third-Party Risk Management* |

| Theme | BCBS Principle | UK Supervisory Authorities |
|---|---|---|
| **Incident Management** | Banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption, considering the bank's risk appetite, risk capacity and risk profile. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents. | The supervisory authorities stated that, in addition to developing policy proposals, they would be drawing together existing policy material which is relevant for the operational resilience of firms and FMIs. When considering other policies such as operational risk and business continuity planning, firms and FMIs should consider how the application of these policies support the delivery of important business services. |
| **ICT Including Cyber Security** | Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programs that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations. | The UK supervisory authorities intend to adopt ICT-related rules that are in line with the European Banking Authority (EBA) guidelines on ICT and security risk management. |

## How We Help Companies Succeed

Protiviti's financial services industry experts help organizations demonstrate and improve resilience through a robust testing program, building upon 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 and issues 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 extreme but plausible scenarios tested regularly?

Additionally, we partner with organizations to develop their overall operational resilience internal audit plans, incorporate operational resilience into existing audits, and provide assurance over the operational resilience program.

## Contacts


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

**Kim Bozzella**
Managing Director, Technology Consulting Financial Services Industry Leader
+1.212.603.5429
kim.bozzella@protiviti.com

**Andrew Retrum**
Managing Director, Global Operational Resilience Leader, Technology Consulting
+1.312.476.6353
andrew.retrum@protiviti.com

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

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

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