protiviti®
Face the Future with Confidence

Regulatory Drumbeat on Operational Resilience Grows Louder with Fed Paper on 'Sound Practices'

November 5,
2020

U.S. federal bank regulatory agencies have issued a much-anticipated paper on operational resilience, adding their voices to the chorus of global watchdogs calling on firms to enhance their resilience capabilities to wide-scale disruptive events before they significantly affect consumers, other businesses and the economy. The Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation (the agencies) released the paper on October 30.

The paper, titled "Sound Practices to Strengthen Operational Resilience," does not revise the agencies' existing rules or guidance, or propose any new mandates. Rather, it draws from existing regulations, guidance, statements and common industry standards to create a set of practices for the largest and most complex domestic firms. The suggested practices are written specifically for U.S. banks with more than $250 billion in total consolidated assets or more than $100 billion in total assets with $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets or average off-balance-sheet exposure. The agencies contend that these practices can help large institutions protect critical operations and core business lines from all major hazards, including technology-based failures, cyberattacks, natural disasters and third-party failures.

Practices for Building Resilience

Consistent with existing regulations and guidance, the agencies offer numerous practices to promote sound and effective governance, operational risk management, business continuity management (BCM) and third-party risk management. Practices on conducting effective scenario analysis are also covered in the paper.

On governing resilience, the paper addresses the board and senior management's roles in overseeing and implementing a resilience program, including setting the firm's risk appetite and articulating its tolerance for disruption. These strategies align with Protiviti's recently published views on how the C-suite and the board can drive operational resilience.

Regarding BCM, the paper stresses the importance of business continuity plans in the management of market-and enterprise-wide stresses and idiosyncratic risks. It also suggests various practices to mitigate third-party risks, including prioritizing third-party dependencies, monitoring vendor performance against service requirements, and identifying substitute services.

Finally, the paper delves into practices on maintaining secure and resilient information systems, surveillance and reporting of operational risks, and cyber risk management (Appendix A of the paper).

Our First Take on the Proposals

To date, the most significant effort by any financial regulator to create formal guidance around operational resilience has come from the United Kingdom, where supervisory authorities, led by the Bank of England, issued a series of coordinated consultation papers on the subject in July 2018 and December 2019. Most recently, in early August 2020, the Basel Committee on Banking Supervision released a consultative document that proposed a pragmatic yet flexible approach to operational resilience, one intended to be principles-based.

Compared to the papers issued by the U.K. supervisory authorities and the Basel Committee, there are some minor (yet notable) differences in the agencies' verbiage and definitions of key operational resilience terms. For example, the agencies' definition of operational resilience includes terms that have not appeared in other previously published definitions. Operational resilience, according to the agencies, is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard.

"Critical operations" and "core business lines" replace the U.K. authorities' preferred term of "important business services and processes." While subtle, the divergence may challenge some firms looking for regulatory alignment on what exactly is considered core, critical or important when it comes to business services. Also, judging by the definitions put forth, the agencies appear to take a top-down approach in how they view firms' resilience. In other words, they mostly address the topic from the standpoint of financial stability and a firm's viability, whereas the U.K. supervisory authorities' papers focus more on customer harm.

The phrase "tolerance for disruption" is used 22 times throughout the agencies 14-page long paper. Its significance to the agencies is clear, although the definition put forth is vague:

> *Tolerance for disruption is determined by a firm's risk appetite for weathering disruption from operational risks considering its risk profile and the capabilities of its*

supporting operational environment. A firm's tolerance for disruption is informed by existing regulations and guidance and by the analysis of a range of severe but plausible scenarios that would affect its critical operations and core business lines.

The vagueness of this definition is particularly striking when one considers the fact that the U.K. regulatory authorities dedicated a paper to dissecting the concept of impact tolerance, a term the authorities defined as "the maximum tolerable level of disruption to an important business service." The term has been heavily discussed since July 2018, with industry leaders and regulators considering various definitions and approaches. In its most recent paper, the U.K. supervisory authorities offered some flexibility in determining impact tolerances, proposing that, where relevant, institutions may decide also to include metrics other than time, such as volumes and values, to determine their impact tolerances.

Another point worth noting is the decision by the agencies to focus on the largest institutions. This is not unexpected, given their ongoing scrutiny of payments clearing and settlement activities. However, this is different from the approach of U.K. regulators, which have taken a much broader view of firms that must address operational resilience. This is yet another indication that the agencies have taken a systemic approach to resilience, while the U.K. regulators are looking at the issue from the perspective of harm at the customer level.

In addressing cyber risk management, the agencies both highlight and contrast the clear overlap between cyber resilience and broader resilience concepts. While cyber events can certainly trigger interruption in critical operations, the paper makes it clear there are broader considerations beyond the cyber-resilience sound practices outlined in the appendix.

Finally, the agencies direct firms to identify their critical services and operations in their recovery or resolution plans (RRP) and to use the RRP plans for managing and aligning their operational resilience to the most important services. This alignment validates the agencies' decision to focus on the largest firms. While this practice is intuitive, Protiviti has found that using RRP plans to effect resilience can create functional challenges that, in some cases, would render the RRP documents ineffective. As such, firms may need to align and/or alter their RRP documents so they can be utilized as part of their operational reliance efforts effectively.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

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

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

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

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

protiviti®