Sound Practices to Strengthen Operational Resilience Explanatory Note

Summary: The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation are issuing the interagency paper, "Sound Practices to Strengthen Operational Resilience" (sound practices). To help large and complex domestic firms address unforeseen challenges to their operational resilience, the sound practices are drawn from existing regulations, guidance, and statements as well as common industry standards that address operational risk management, business continuity management, third-party risk management, cybersecurity risk management, and recovery and resolution planning. Specifically, the agencies set forth sound practices drawn from existing regulations and guidance for individual national banks, state member banks, state nonmember banks, savings associations, U.S. bank holding companies, and savings and loan holding companies that have average total consolidated assets greater than or equal to (a) $250 billion or (b) $100 billion and have $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance-sheet exposure.

I. Background

The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation, (collectively, the agencies) are issuing the interagency paper "Sound Practices to Strengthen Operational Resilience" (sound practices). Over the last decade, the agencies have instituted various reforms aimed at enhancing the prudential framework and improving the financial resilience of domestic firms and the financial system more broadly. These reforms – which included stronger capital and liquidity

requirements as well as enhanced recovery and resolution mechanisms – reduce the likelihood and severity of a firm's failure.

Notwithstanding these improvements to financial stability, firms in recent years have experienced significant challenges from a wide range of disruptive events, including technology-based failures, cyber incidents, pandemics, and natural disasters. Such events, combined with a growing reliance on third-party service providers, expose firms to a range of operational risks. These risks underscore the importance for firms to strengthen their operational resilience, which the sound practices describe as the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. These disruptions could include, but are not limited to, technology-based failures, cyber incidents, natural disasters, and third-party failures.

The agencies recognize that technological developments have provided firms with new tools, such as cloud-based computing resources, to strengthen their operational resilience to support a firm's operational resiliency. Nonetheless, the agencies view the risk of a significant operational disruption as material and that such a disruption could jeopardize these hard-won gains in financial stability and resilience. While efforts to strengthen operational resilience may not prevent a disruption from materializing, a pragmatic, well-constructed approach to operational resilience can help minimize the adverse effects of an operational disruption and enhance a firm's ability to withstand it.

The sound practices bring together existing regulations and guidance as well as common industry standards to provide a comprehensive approach that firms may use to strengthen and maintain their operational resilience. In this approach effective governance grounds the sound practices. Robust operational risk and business continuity management anchor the sound

practices, which are informed by rigorous scenario analyses and consider third-party risks. Secure and resilient information systems underpin the approach to operational resilience, which is supported by thorough surveillance and reporting. The sound practices do not amend, expand, or alter the agencies' existing regulations or guidance.

Given the significance and technical nature of cybersecurity risk, which constitutes one of the most important types of operational risk, Appendix A provides a separate collection of sound practices for the management of cyber risk. Appendix B provides a glossary of definitions used in the sound practices.

The issuance of these sound practices facilitates the ongoing discourse with the public on operational resilience. In the coming months, the agencies intend to convene discussions with the public on further steps to improve operational resilience. Continued dialogue with the public will allow the agencies to further refine their approach to support the operational resilience of firms. In these forthcoming discussions, the agencies will be particularly interested in discussing ways in which the largest and most complex firms can improve the operational resilience of critical operations and core business lines of a firm's material entities and how they and supervisors can measure operational resilience and firms' progress toward achieving it. Given that many of these firms have extensive cross-border activities, the agencies will seek to minimize the potential for market fragmentation and to align best practices for operational resilience.[1] The agencies may update the sound practices to reflect input from these discussions.

[1] To further strengthen practices on operational resilience, the Basel Committee on Banking Supervision (the Committee), in consultation with the agencies, published in August 2020 a principles-based approach to improving operational resilience. Similar to the approach provided in the sound practices, the consultative paper builds on updates to the Committee's Principles for the sound management of operational risk and draws from previously issued principles on corporate governance for banks, outsourcing, business continuity, and operational risk.

Applicability

Although operational resilience is important to all firms, the sound practices are directed to the largest and most complex domestic firms. This paper describes sounds practices drawn from existing regulations and guidance for individual national banks, state member banks, state nonmember banks, savings associations, U.S. bank holding companies, and savings and loan holding companies that have average total consolidated assets greater than or equal to: (a) $250 billion, or (b) $100 billion and have $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance-sheet exposure.[2] This paper does not set forth any new regulations or guidance for these firms, but rather it brings together the existing regulations and guidance in one place to assist in the development of comprehensive approaches to operational resilience.

The agencies acknowledge that operational resilience is important to firms of all sizes, and that any firm may find elements of the sound practices useful as it considers operational risk and resilience challenges. However, because the sound practices emphasize critical operations of a firm's material entities, which generally are characteristic of large firms, the sound practices paper is not written to a smaller firm audience. These smaller firms continue to be subject to existing regulations, guidance, interagency statements, and common industry standards related to operational risk and operational resilience.

A key objective of the sound practices is promoting harmonization across international and domestic frameworks regarding operational resilience, and the agencies are aware of similar

[2] This includes U.S. domestic firms that are considered 1) Global Systemically Important (GSIB) Bank Holding Companies, 2) Category II bank holding companies, 3) Category II savings and loan holding companies, 4) Category III bank holding companies, or 5) Category III savings and loan holding companies. It also includes GSIB depository institutions supervised by the OCC, Category II national banks and Federal savings associations, and Category III national banks and Federal savings associations (*see, e.g.*, 12 CFR 3.2 and 50.3; 12 CFR **324.2).** It does not apply to U.S. intermediate holding companies.

international efforts to improve operational resilience. The agencies also note that a foreign firm's activities within the U.S. could pose similar risks to U.S. financial stability comparable to those posed by similarly sized domestic organizations.

For further information contact: Carlos Sosa, Lead Financial Institution Policy Analyst (202) 503-7294; Julia J. Philipp, Lead Financial Institution Cybersecurity Policy Analyst, (202) 452-3940; Don R. Adams, Senior Supervisory Cybersecurity Analyst, (202) 452-3730; Andrew Willis, Lead Financial Institution Policy Analyst, (202) 912-4323; or Brendan Rowan, Senior Financial Institution Policy Analyst, (202) 475-6685, Division of Supervision and Regulation; or Christopher Callanan, Senior Counsel, (202) 631-0188, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets, NW., Washington, DC 20551.