November 6, 2020

Via Electronic Submission

Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel, Switzerland

Re: *Consultative Document: Principles for operational resilience*

Ladies & Gentlemen:

The Bank Policy Institute[1] and the American Bankers Association[2] appreciate the opportunity to respond to the August 2020 consultative document (the "Proposal") issued by the Basel Committee on Banking Supervision (the "Committee"), *Principles for operational resilience*, which would articulate a principles-based approach to improving operational resilience for the purpose of strengthening the ability of banks to withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets, such as pandemics, cyber incidents, technology failures or natural disasters.[3]

Operational resilience is an important priority for all participants in the global financial system, and an integral part of how banks and other financial institutions and market utilities ensure they can continue to serve customers, clients, and markets in the face of operational disruption. For this reason, we welcome international supervisory efforts to assess the existing operational resiliency of banks, identify evolving best practices and opportunities for public/private coordination that support operational resilience, and establish consistent global standards for the promotion of operational resilience both within firms and across the financial system.

We also believe strongly that, as a supervisory matter, operational resilience is best addressed through a framework that is based on broad principles and assesses the extent to which a firm has built a

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 The American Bankers Association is the voice of the nation's $18.6 trillion banking industry, which is composed of small, regional and large banks. Together, America's banks employ more than 2 million men and women, safeguard $14.5 trillion in deposits and extend more than $10.5 trillion in loans.

3 *See* Basel Committee on Banking Supervision, *Consultative Document: Principles for operational resilience* (Aug. 2020) [hereinafter the "Consultative Document"].

program that is effective at identifying potential threats and promoting the firm's ability to recover from, and otherwise remain resilient in the face of, potential disruption. This is especially important given the dynamic and multi-dimensional nature of potential disruptive threats, which makes a bank's capacity to plan for, respond, and adapt to evolving threats fundamental to operational resilience as an outcome. We thus support the extent to which the Proposal seeks to articulate foundational principles for operational resilience and avoid imposing specific and prescriptive mandates. To that end, this letter identifies a range of suggestions that we believe would further align the Proposal with its stated principles-based approach.

I. Operational resilience is an important priority for both banks and other financial institutions, and banks have devoted significant efforts, both individually and through collaborative efforts of the public and private sectors, to understand, assess and improve operational resilience across the financial system.

Building and maintaining operational resilience has long been a priority for banks, given the importance of resilience to a bank's ability to continue to serve markets and customers notwithstanding operational disruption. For this reason, banks have long been at the forefront of larger corporate efforts to continuously enhance and improve their operational capabilities and readiness, including through business continuity planning ("BCP"), operational risk management, and cybersecurity investment and innovation. This is not simply a matter of regulatory compliance; rather, it has been and remains good business and sound risk management for banks to focus and prioritize on building and sustaining their operational resilience in the face of potential disruption. Indeed, much of this past work enabled firms and the broader industry to continue to operate throughout the ongoing COVID-19 pandemic despite unforeseen interruptions to staffing, increased demands on technology systems, and disruptions to supply chains and outsourcing plans as countries instituted lockdowns and restricted the movement of essential employees. Notably, the challenges and threats against which banks must remain resilient are themselves highly dynamic and subject to constant change and evolution, such that resilience is best understood not as an obtainable "end state," but rather a process of continuous improvement and adaption to address threats to resilience as they are identified and evolve.

Reflecting this priority, and in addition to their individual efforts to enhance operational resilience, banks in recent years have also undertaken a range of extensive and maturing collective efforts aimed at enhancing the operational resilience of both individual firms and the broader sector, often in partnership with the public sector. In the U.S. for instance, such work has included exercises and programs to explore systemic risks of the global interconnected financial system, dedicated initiatives designed to identify, assess and prioritize risks to significant market segments (e.g., global wholesale payments), data vaulting standards to improve resiliency and recovery, and operational response groups to facilitate information sharing of cyber threat indicators across the nearly 7,000 global members of the financial industry's information sharing organization.[4]

---

[4] This work includes, for example: (i) participation in the "Hamilton" series of exercises which, led by the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), the Financial Services Sector Coordinating Council ("FSSCC") and the U.S. Treasury Department under the auspices of the U.S. Financial and Banking Information Infrastructure Committee ("FBIIC"), explore the systemic risks to the banking system from significant incidents such as a pandemic or destructive malware attack; (ii) formation and operation of Sheltered Harbor, a non-profit subsidiary of the U.S. Financial Services Information Sharing and Analysis Center ("FS-ISAC") devoted to coordinating the development of industry standards and supporting infrastructure to help financial institutions back up critical account data on a nightly basis; and (iii) establishment of the Financial Systemic Analysis & Resilience Center ("FSARC"),

Importantly, the collaborative and multi-dimensional nature of these collective industry efforts reflect the inherent complexity of operational resilience in the context of a broader financial system in which firm-specific efforts are necessary, but not sufficient. Given the interconnected nature of the global financial system, operational resilience depends not only on banks' internal preparedness and capabilities, but also that of other key market participants, including both private and government-operated financial market utilities and other key nodes of the financial system. Operational resilience initiatives must therefore also recognize the unique roles that regulators, nonbank financial providers, insurers, and technology suppliers play alongside banks in ensuring stability across the financial sector and the broader economy.

Finally, we note that the response to the recent and ongoing COVID-19 pandemic has affirmed the importance of flexibility and adaptability for financial institutions in maintaining an operational resilience and cybersecurity readiness posture that protects customers and ensures the continual functioning of the global financial system. Despite the nearly unprecedented nature of the pandemic and its global scope, firms were successfully able to quickly implement new loan programs and facilitate government stimulus initiatives to support customers and the broader economy, while simultaneously dealing with the impact of the pandemic on society by implementing social distancing measures in retail branches and call centers, and shifting the majority of the workforce to a remote work environment. By leveraging existing processes and plans—such as BCP, cybersecurity and technology resilience work—firms were able to quickly and efficiently adjust their operations to meet these new demands as the impacts of the pandemic continued to spread geographically. While firms are continuing to assess the lessons learned throughout this experience, their existing planning efforts and testing regimes provided a solid foundation from which to support needed adjustments in a timely fashion. Although the COVID-19 pandemic represents only one of many different types of potential disruptions for which banks must prepare, and its operational challenges were not sudden and abrupt in nature, banks' response to the pandemic's operational challenge nonetheless demonstrates the value of existing processes and plans that can be flexibly leveraged when disruption inevitably occurs.

II. We support the Committee's work to foster international coordination and consistency in standards for operational resilience, which is crucial in ensuring that global banks are subject to consistent and aligned regulatory or supervisory expectations in each jurisdiction in which they operate.

We particularly appreciate the Committee's leadership in fostering a robust public policy debate concerning how best to assess and supervise operational resilience and, through its role as an international standard-setting body, working to create consensus, consistency, and collaboration among national supervisors on this important policy issue. Given the global scope of many banks and the markets and financial systems in which they operate, it is crucial that any supervisory standards for operational resilience be consistent and harmonized across different jurisdictions—an objective that the Committee's work can and should advance. Ensuring that any standards are appropriately developed and harmonized at an international level would bolster market confidence, allow for better identification and mitigation of cross-border disruptions, and better position both firms and the industry more broadly to reduce risks. Doing so would also avoid the significant risk for potential fragmentation in standards across different jurisdictions,

---

which was created in 2016 by a consortium of financial services firms to develop a confidential risk register that reflects technological and operational threats that have the potential to cascade from one financial institution through the entire sector. Part of the FSARC's mission is to facilitate coordination among banks, the Department of Homeland Security, U.S. Treasury and the U.S. intelligence community to better identify, prioritize, and defend critical infrastructure against an attack and support the operational resilience of the financial sector.

which would be particularly harmful in the context of systemic resilience because nearly all systemically important sectors and activities are international in nature.

As individual jurisdictions begin to develop and implement operational resilience standards that would apply locally, the importance of international coordination will only increase.[5] This work will also help ensure the effective and efficient use of resources to support desired operational resilience improvements, as well as a global policy development process for operational resilience that is iterative, supported by continued dialogue among industry and regulators, and appropriately coordinated across international supervisors.

Importantly, operational resilience across the financial system depends not only on banks but also other key participants in the system, including nonbank financial providers, insurers, technology suppliers and other key third-party service providers. Recognizing that the Committee's remit is limited to banks, we nonetheless encourage the Committee to coordinate with other international standard-setting bodies in support of a broad policy response that covers not only banks, but also financial market utilities, insurance providers, and other key participants.

III. We support the principles-based nature of the Proposal, as standards for operational resilience should ensure financial institutions have the necessary flexibility and agility to achieve operational resilience.

Given the dynamic and multi-dimensional nature of potential disruptive threats, change and adaptability is fundamental to operational resilience as an outcome. An appropriately risk-based approach to operational resilience is likely to entail meaningfully different approaches across different types of firms and businesses, and specific and prescriptive standards are likely to become quickly outdated or irrelevant, resulting in a misallocation of resources and possibly diverting attention away from greater, emerging risks. Thus, as a supervisory matter, operational resilience appropriately requires a framework that is based on broad principles and assesses the extent to which a firm has built a program that is effective at identifying potential threats and promoting the firm's ability to recover from, and otherwise remain resilient in the face of, potential disruption.

For these reasons, we support the overall approach taken by the Committee in the Proposal, in that it seeks to articulate foundational principles for operational resilience but attempts to avoid imposing specific and prescriptive mandates regarding the ways in which every bank's operational resilience program must be defined and operated. We also support the ways in which the Proposal seeks to encourage an approach to operational resilience that is proportional and risk-based in nature, recognizing that the size, business model and risk profile of banks may vary significantly. As a matter of approach, the Proposal's stated focus on *principles* is crucial, as operational resilience cannot be reduced to a standardized test that discourages or disincentivizes the kind of proactive, creative, and continually-adaptive management attention that effective operational resilience requires, since it would likely promote a "check-the-box" approach to supervisory assessment and bank compliance. To that end, we outline below

---

5 *See, e.g.,* Bank of England and Financial Conduct Authority, *Building the UK financial sector's operational resilience* (December 2019); European Commission, *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure* (December 2019); Monetary Authority of Singapore, *Ensuring Safe Management and Operational Resilience of the Financial Sector* (April 2020); International Organization of Securities Commissions, *Principles on Outsourcing* (May 2020).

a range of suggestions that we believe would better align the Proposal with its stated principles-based approach.

IV. The Proposal would appropriately focus on disruption that is material to a bank's operational viability or to financial stability.

The proposal would define *operational resilience* as "the ability of a bank to deliver critical operations through disruption," and for this purpose would capture "activities, processes, services and their relevant supporting assets the *disruption of which would be material to the continued operation of the bank or its role in the financial system*."[6] We support the Proposal's definitional focus on disruption that could pose significant risk to a bank's continued operations or to its role in the financial system (i.e., financial stability). We believe that these are the appropriate risks at which supervisory expectations for bank operational resilience should be aimed and consistent with the scope of the Committee's remit.

V. The Proposal's reference to recovery and resolution planning concepts and processes as defined by the Financial Stability Board ("FSB") is helpful, but should not be used to require banks to automatically tie their definitions of "critical operations" for operational resilience purposes to "critical functions" for recovery and resolution planning ("RRP") purposes, and the Proposal should otherwise make clear that banks may consider whether, but are not required, to directly incorporate or replicate aspects of other supervisory frameworks into their operational resilience program.

While we whole-heartedly endorse operational resilience principles that *permit* banks to leverage other supervisory frameworks, processes, and concepts into their operational resilience efforts where they conclude this will support or enhance those efforts, we are concerned that several aspects of the Proposal might be construed as *requiring* banks to do so, which would be both unduly prescriptive and potentially counterproductive for several reasons.

First, we are concerned that the Proposal's definition of "critical operations" might be construed as *automatically* deeming all "critical functions" for RRP purposes to also be "critical operations" for operational resilience purposes, which is neither necessary nor appropriate.[7] While there are obviously conceptual similarities between certain aspects of RRP and operational resilience, there also can be important differences, as RRP involves unique objectives and considerations (e.g., with respect to timing). For that reason, we suggest that the relevant definition should be revised to encourage banks to *consider* their critical functions for RRP purposes in developing operational resilience programs, while still leaving banks with significant flexibility in how, and at what level of granularity, they define critical operations for

---

6 Consultative Document at paragraphs 12, 13 (emphasis added).

7 *See* Financial Stability Board, *Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services* (2013). According to the FSB, "critical functions" are defined as "activities 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." *Id.*

operational resilience purposes. This more flexible approach would better promote an integrated and holistic view of operational resilience across the firm.

Second, in defining operational resilience, paragraph 12 of the Proposal states that a bank should take into account "its overall risk appetite, risk capacity, and risk profile," referencing (in a footnote) the definition of those three terms under the Committee's 2015 *Corporate governance guidelines* and the FSB's 2013 *Principles for an effective risk appetite framework*. Although the precise definition of those terms in those contexts are helpful and may be considered in framing how a bank approaches operational resilience, those definitions are unlikely to be entirely fit for purpose in the operational resilience context, where the relevant risk considerations at a sector or financial system level involves a wide range of stakeholders and interdependencies, going well beyond traditional risk appetite considerations at an individual firm level.

Third, we note that other aspects of the Proposal make specific reference to RRP processes and determinations, or concepts derived from other supervisory frameworks. This includes:

- Paragraph 10 of the Proposal, which states that "banks should consider whether their operational resilience efforts are appropriately harmonised with the stated actions, organisational mappings, and definitions of critical functions and critical shared services contained in their recovery and resolution plans as specified in the Financial Stability Board's (FSB) Recovery and Resolution Planning framework";
- Principle 2 of the Proposal, which states that banks "[f]or operational resilience purposes, appropriate coordination with … recovery and resolution planning … frameworks may yield greater harmonisation in delivering a consistent approach to operational resilience across the enterprise";
- Principle 3 of the Proposal, which states that banks should "consider whether their operational resilience efforts are appropriately harmonised with the bank's business continuity plans for the delivery of critical operations and critical third-party services contained in their recovery and resolution plans"; and
- Principle 4 of the Proposal, which states that banks "should consider whether their operational resilience efforts are appropriately harmonised with the organisational mappings of critical operations and critical third-party services contained in their recovery and resolution plans."

Although each of these references appear intended to *permit* but not *require* banks to leverage aspects of other frameworks—flexibility that is useful and we therefore support—we are concerned that the language may be sufficiently ambiguous that, in local implementation, it could be misconstrued as imposing more prescriptive and mandatory requirements (e.g., that banks must synchronize their operational resilience and RRP frameworks), which is problematic for the reasons described above. To mitigate that risk, we suggest that the Committee make clear, throughout any final version of the Proposal (including the sections identified above), that no such requirement is imposed, but rather banks retain significant flexibility in determining whether and how to leverage RRP or other processes and determinations for operational resilience purposes.

VI. The Proposal should also carefully distinguish and differentiate between operational resilience at a sector level and resilience at a firm level and, in proposed Principle 5 and elsewhere, acknowledge that addressing operational resilience at a financial system level requires broad collaboration between the public and private sectors.

Although the Proposal generally speaks of operational resiliency risks to an individual firm and to the broader financial system collectively, and would articulate the same principles for each, it is important to emphasize that these resiliency goals—and the means necessary to achieve them—vary in significant ways. Although firms can and should identify and assess operational resiliency risks to their own viability and safety and soundness, resilience at a sector or financial system level is inherently multi-dimensional, demanding a clear understanding across all relevant firms and the public sector of what is systemically important, and what outcomes are necessary. Resiliency at a sector or financial system level can be informed and supported by individual firm action. Ultimately, however, it must rest upon collective and collaborative decision-making and action by not only banks, but also regulators, nonbank financial providers, insurers, technology suppliers, and other key constituents and stakeholders across the financial system. Moreover, given the role that critical third parties and third-party dependencies play in important parts of the financial system, a similarly broad, system-level view and approach is needed to ensure that these aspects of the financial system support, rather than undermine, operational resilience.

For these reasons, collaborative forums can and should serve as a primary means by which (i) operational resilience at a sector and financial system is assessed, and (ii) the actions that individual firms should take in furtherance of that resilience are identified. Because international regulators can and should play an important role in convening key stakeholders and providing clarity in this area, we suggest that the Committee explicitly acknowledge these differences and their implications in any final version of the Proposal. For similar reasons, we also suggest that the Committee acknowledge, both in general and in the context of proposed Principle 5, the equal importance of public and private sector collaboration in evaluating and addressing the role of third parties and third-party dependencies in achieving operational resilience.

VII. The Proposal should acknowledge the complementary importance of taking into account and prioritizing operational resilience efforts that prevent or limit disruption.

While it is critically important that firms' operational resilience efforts take into account the possibility of disruption, true operational resilience reflects a holistic effort by banks to reduce not only the impact of disruption, but the probability of disruption as well. This is particularly true at the level of firm prioritization and resource allocation, where operational resilience is best served by banks' carefully assessing and balancing both of these goals. Thus, for example, as a firm considers how best to allocate operational resilience resources, it *should* matter which types of disruptions or scenarios are more plausible than others. Similarly, it is entirely possible that there may be cases where a bank cannot meet its resilience objective for a particular service, system or function, yet its operational resilience may be well served by a strong focus on limiting the probability of disruption, rather than improving its ability to recover from that disruption alone. We suggest that, in any final version of the Proposal, the Committee underscore the importance of assessing and addressing prevention and recovery holistically, with a view towards allocating firm resources and attention to investments and activities that provide the most efficient and effective benefits to the overall operational resilience of a firm.

VIII. The Proposal appropriately acknowledges that measurement methodologies and metrics for operational resilience are nascent, untested, and merit further study.

We agree with the Committee's statement that "measuring a bank's 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." While quantitative metrics can be useful in certain areas of regulation and supervision, potential measurement tools for operational resilience are relatively new and untested, and the dynamic and complex nature of operational resilience means that it is unlikely there will be any single metric of "sufficient" operational resilience that will be appropriate in all cases. Moreover, any reduction of the complexities of operational resilience to specific metrics likely would not promote a complete or accurate picture of a bank's operational resilience.

There is, as well, the risk that quantitative metrics—should they serve as a core measure of compliance with supervisory expectations—could create incentives that are in tension with the Proposal's policy aims. Specifically, if these types of metrics were implemented in a way that does not grant banks appropriate flexibility and discretion when deploying them within their operational resilience framework, these metrics could lead supervisors and banks to reduce complex operational challenges to standardized measures, and focus their operational resilience efforts on managing to those standardized measures. Such efforts would come at the cost of tailored, dynamic efforts capable of achieving operational resilience aims in a constantly changing environment.

* * * * *

The Bank Policy Institute and the American Bankers Association appreciate the opportunity to comment on the proposal. If you have any questions, please contact Chris Feeney at (202) 589-2437 or by email at Chris.Feeney@bpi.com, or Paul Benda at 202.663.5256 or PBenda@aba.com.

Respectfully submitted,

Christopher F. Feeney
President of BITS and Executive Vice President
Bank Policy Institute

Paul Benda
Senior Vice President Risk and Cybersecurity Policy
American Bankers Association