BANK POLICY INSTITUTE

January 8, 2021

Financial Stability Board
Via Electronic Mail to fsb@fsb.org

Re: Comments in Response to the Financial Stability Board discussion paper: *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*

To the Financial Stability Board:

The Bank Policy Institute[1], through its technology policy division known as BITS, appreciates the opportunity to comment in response to the FSB discussion paper, "*Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships"*[2], and to reply to the dialogue-facilitating questions posed within. Published in November 2020, the discussion paper compiles the results of a prior FSB survey examining the regulatory and supervisory environment overseeing third party relationships with financial institutions. In doing so, the paper provides relevant background and context for a continuing dialogue among supervisory authorities, financial institutions, and third parties.

Managing third-party relationship risk is not new to the financial services industry. However, in recent years the pace of outsourcing has accelerated, and the scope of services has expanded, due in part to the rapid digitalization of services. Financial institutions are drawn to the ability to quickly adapt and augment their core and peripheral operations via third-party providers whose products and services offer cutting-edge technology solutions that can solve a variety of business challenges and directly benefit a partnering institution's customers. Third-party service providers' benefits are accompanied by challenges for institutions related to identifying, managing, and mitigating associated risks. Regulators also face challenges with balancing institutions' desire for improving customer experience through innovation, agility, and operational benefits, with regulators' duties to monitor the safety and soundness of the global financial system.

To address these concerns – and in response to the dialogue-facilitating questions posed by the FSB discussion paper – we offer comments addressing baseline recommendations for the global third-party risk management regulatory landscape. Once established, we

[1] See Annex A for a description of the Association

[2] FSB, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships (November 9, 2020), available at: https://www.fsb.org/wp-content/uploads/P091120.pdf

will focus on the key challenges faced by financial institutions and where available, solutions for ongoing collaboration. Finally, we will discuss adjustments made and lessons learned from the COVID-19 pandemic as applied to third-party risk management.

1. **We encourage supervisory authorities to set out sufficiently streamlined and harmonized guidance on how financial institutions should manage their outsourcing and third-party relationships.**

Regarding the regulation of third-party relationships in the financial system, we encourage regulators to apply flexible, objectives-based principles that enhance resiliency and responsiveness within the sector wherever possible. These principles should align to existing regulatory frameworks to avoid duplicative or conflicting expectations and enable firms to identify opportunities for enhancements related to their third-party resilience oversight programs.

In addition to coordinated and streamlined regulation, regulators should ensure that terminology spanning various regulatory jurisdictions is clear and consistent. To realize the full potential of their partnerships with third parties, financial institutions need to be confident in their understanding of how those relationships are treated on a cross-border basis. Definitions of terms such as “outsourcing” and “third-party” regularly vary amongst supervisory regimes. A common global understanding of key terms would help shape consistent expectations between regulators and financial institutions, in addition to better positioning regulators and supervisors to collect reliable information in support of systemic risk monitoring.

Beyond harmonization of terminology and definitions, it is also critical for regulators and institutions to accurately identify and categorize third-party providers according to their risk profile and operational model, and to recognize that these differences are material to how they should be overseen. Services provided to third parties that are regulated do not pose the same risks to financial institutions as unregulated third parties. It is also necessary for regulators to differentiate between intra-group outsourcing and external outsourcing on the basis that risks can be less pronounced based on the control and influence an entity has over the intra-group entity. Regulators should seek to ensure that the relevant legal entity is able to show that it is complying with the regulations and standards of the region in which it operates, regardless of the geographic location of the technology or risk management. While intragroup outsourcing on a cross-border basis can reduce overall risk for an institution and improve operational resilience, the implementation of localized systems, data, and processes may reduce the realization of the desired benefits.

We encourage regulators to recognize existing effective private sector approaches to third-party management and due diligence processes and tools to evaluate third party risk. The third-party service provider marketplace operates globally and recognizing existing effective approaches will help to develop coordinated regulatory regimes that reduce cross-border friction at every opportunity.

2. **Dialogues among financial institutions, third parties, and supervisory authorities should focus on addressing the following challenges: cross-border interoperability; supply chain oversight; cloud regulatory treatment; concentration risk; audit and information access rights; and supervisory overlap.**

The 21st century global financial marketplace demands both maximum stability and innovation from its participant institutions. Customers around the world expect frictionless, uninterrupted access to their financial resources even as the world changes daily around them. To achieve this, financial institutions have matured internally and have sought to leverage innovative products and services from external providers to augment their existing businesses. While keeping up with the pace of innovation, financial institutions have also recognized a need to manage new risks posed by their third parties and outsourced partners. In response to the first two questions posed by the FSB discussion paper, we highlight some of the most pressing challenges and suggest solutions for further discussion.

Cross-border interoperability: Regulators are increasingly active participants in most, if not all, of the international forums bringing together regulators and firms to discuss key issues, including third-party risk. Regulators are working to align to core principles however, local jurisdictions continue to develop their own requirements. For example, data localization proposals are proliferating. In response, individual jurisdictions are responding with their own measures to assert jurisdictional sovereignty or entering bilateral trade agreements to create permissible flows of data between countries. In some instances, broader trade agreements are creating regional frameworks for the exchange of data and protection of privacy. Yet regardless of the response implemented by an individual jurisdiction, there is little interoperability between approaches. Without unified global effort to achieve coordinated and stable outsourcing requirements that are harmonized across jurisdictions, institutions are left to navigate a fragmented regulatory landscape that threatens to make third-party oversight more complex and reduces operational resilience.

Regulations should be developed with the understanding that the marketplace for financial services third-party outsourcing is not confined to individual jurisdictions, and prudential regulatory regimes should reflect this reality. By committing to a principle of cross-border regulatory coordination, supervisors/regulators and industry will be able to work on establishing a universal understanding of a financial institution's risk exposure and potentially broader industry risk exposure. Coordinated interoperability also helps regulators and firms to prioritize resources and focus on risks of greatest concern. One way to meet this challenge would be for regulators to publicly accept an assessment framework that incorporates existing standards like NIST or ISO as a part of their examination processes. For example, the FSSCC-developed Cyber Risk Institute's Financial Services Cybersecurity Profile[3] is an assessment framework that satisfies this

[3] The CRI Financial Sector Profile (Profile), formerly known as the FSSCC Cybersecurity Profile, was developed as a collaborative effort between 150 financial firms, 300+ bank representatives and input from multiple regulatory agencies and experts. The result is a unified harmonized approach to cyber security assessments that can be used

suggestion. By mapping regulatory requirements to a series of diagnostic statements organized around well-established standards, we can improve regulators' abilities to make cross-industry comparisons from a common baseline and increase compliance efficiency.

Supply chain oversight: Another challenge that financial institutions encounter is risk emanating from visibility into an up or downstream supply chain, both prior to and throughout a third-party relationship. Even under conditions of maximum transparency, the third party may have its own existing relationships (also known as "nth party") that create risk outside the appetite or requirements of a financial institution or its regulators. The inability of an institution to revise or renegotiate the terms of a service agreement with an nth party vendor or supplier with which it is not in privity can impact an institution's ability to mitigate against risk and meet its compliance objectives. To overcome this challenge, regulators should support existing industry tools like voluntary certification or standardized approaches to ensure that compliance expectations are proportionate to the risk exposure.

Cloud regulatory treatment: The practice of outsourcing various financial institution operational components to cloud environments has trended from leading-edge to normal, perhaps even prudent, in recent years. A flexible regulatory model that allows for the ability to distinguishbetween varying types of cloud environments (e.g., SaaS, PaaS, or IaaS) and their accompanying degrees of control, encourages realization of the benefits institutions seek to derive without ignoring the disparate degrees of risk. Regulators should also explore the appropriate role that global regulators can play in overseeing cloud providers and ensuring cross-border interoperability where local regulators, by nature of their intra-border limits, would be more likely to curtail these activities through the course of oversight.

Concentration risk: Institutions may also encounter challenges in the form of concentration of products or services. The ability of the financial institution to navigate concentration risk exposure depends on the degree of dependency to the provider. While financial institutions can be held responsible for managing third-party concentration risks within their own institution, regulatory authorities should still observe for industry-wide concentration risk and discuss any concerns with industry. Within these bounds, regulators should be mindful to balance managing sector-wide risks while understanding that access to certain third-party providers can foster innovation and a lack of access may cause a competitive disadvantage.

We believe the appropriate approach is not to seek the elimination of this risk, but rather that there should be a focus on gaining visibility into concentration risk, building the right security and resiliency capabilities to manage these risks, and that the public and private sector should work together to create an environment which does not stifle the ability to utilize third parties.

---

by the smallest and largest financial services firms: banks, securities, and insurance. Ownership and management of the Profile transitioned from FSSCC to the non-profit Cyber Risk Institute (CRI) in January 2020. The CRI Financial Services Profile can be found at https://cyberriskinstitute.org/the-profile/

Audit and information access rights: Financial institutions can encounter limitations on audit and information access when engaging with third parties. As noted in the supply chain oversight discussion, some of these limitations occur because a third-party has a self-interested business reason for withholding the information (e.g., sensitive or proprietary business information, or asymmetry between the relationship value and the information requested). Other limitations arise because although an institution may be bound by the terms of a contract with a third party, contracts only bind those parties in privity to the agreement and it may be infeasible to extend these obligations to "nth" parties in the third-party vendor's supply chain. Institutions commonly attempt to incorporate risk controls (e.g., auditing or due diligence exercises) into their contract relationships, but negotiation and implementation outcomes related to these extended supply chain relationships can still leave institutions exposed to risk with limited or no readily available remedy. Third parties also run the risk of exposing themselves and their supply chains to overburdening through multiple and duplicative audits all requesting similar information.

Recognizing this, institutions have coalesced around several practices designed to mitigate these concerns and to reduce burden and duplicity on themselves and their third-party partners. These practices include engaging in shared or pooled audits where multiple institutions share a common third party; leveraging third-party certification programs; and utilizing standardized approaches to collecting evaluation data. In this way, the industry is potentially able to reduce some of the obstacles by sharing and reusing non-sensitive information for the collective efficiency and security of the sector.

Still, these industry-developed practices cannot address all access limitations and there may be situations where direct regulatory oversight of a third party is preferred or required. Therefore, where regulators consider direct oversight, they should seek to ensure global coordination and maximum interoperability, as well as proportionality if the third-party is presently regulated by a competent authority.

Supervisory overlap: As previously noted, many third-party services operate on a cross-border basis and the ability of a financial institution to seek out and adopt innovative services benefits greatly from increased global regulatory coordination. Many institutions encounter regulatory challenges in the form of duplicative, conflicting, or burdensome layering of regulatory regimes where a third-party is regulated both prudentially for its own activities as well as separately for its role as a third-party service provider. Regulators should recognize these redundancies and consider whether the risk sought to be mitigated is already addressed as part of the underlying or existing regulatory regime. Doing so will ensure greater consistency and reduce burden on institutions and third parties alike.

3. **The Board appropriately recognizes the complexity that financial institutions encounter when managing third-party risk and acknowledges that all parties involved could benefit from enhanced dialogue, which it should continue to pursue.**

The paper concludes by noting that, "effective cross-border cooperation and dialogue among supervisory authorities as well as the effective application of existing standards and other emerging practices are important to address these challenges and risks."[4] We concur and point specifically to the earlier-discussed challenges as evidence of the need for regulators to ensure that earnest consideration is given to clarity, consistency, proportionality, and coordination. The complexity of the third-party landscape, both in terms of scope of products and services as well as jurisdiction, requires maximum attention to these objectives.

Establishing a successful regulatory regime that functions on a global scale to concurrently encourage regulatory compliance while avoiding the stifling of innovation will require commitment from all parties to maintain an ongoing and earnest dialogue. To achieve this, regulators should consider deploying collaboration tools such as public-private forums where candid exchanges of information and functionality assessments are shared across the policy and supervisory landscape and to covered industry stakeholders. This will enhance ongoing regulatory development by giving regulators specific areas or topics to address without the fear that their consideration could create a less workable regulatory environment. As an example, this could include exercises in respect of concentration risk. In the event of a disruption at a major provider it is vital that the financial industry, including its regulators, have rehearsed some of the potential scenarios and steps required be resilient and operate. Exercises that help all market participants better understand the actions they would need to take and pre-identify risks that could arise as a result would therefore be a useful initial step toward addressing concerns related to systemic concentration.

4. COVID-19 risk management adjustments and lessons learned

BPI and its BITS technology policy division have conducted extensive research on this subject to help understand how its member institutions and affiliate members are navigating the ongoing pandemic. From this research, we can highlight some of the lessons learned and adaptive changes deployed, such as:

- Increased frequency and cadence of monitoring their third-party vendors
- Expansion of pandemic planning in due diligence assessments
- Reconsideration of offshore third-party operations and onshore continuity plans
- Adjustments to electronic due diligence and monitoring due to the inability to conduct onsite audits as a result of travel and personal contact restrictions
- Commitment to scaling resources for the technical challenges of a remote workforce
- Altering information security assessment approaches

Because of their experiences over the previous year, institutions are evaluating their exposure to events through an expandedaperture in terms of risk, impact, and recovery.

[4] Id. at 15.

The timing or practicality of returning to a pre-COVID operating posture is unclear, and firms are actively re-assessing the policy, process, and operating changes they made to ensure those changes, and the accompanying lessons learned, are incorporated on a more permanent basis. Maximizing organizational flexibility, resilience planning, and vendor evaluation remain the core risk management objectives moving forward.

Agility and responsiveness have emerged as paramount considerations for firms in managing operational resilience and assessment of third-party risk. As the triage response component of COVID-19 recedes, firms can take their COVID-augmented resiliency plans forward against the regulatory challenges raised within this ongoing discussion. However, all parties should recognize that while the crisis may eventually fade, the newly identified areas of concern arising from the pandemic should remain an integral focus on an ongoing basis, and with sufficiently-dynamic controls to react to the full spectrum of potential outcomes.

Thank you for the opportunity to respond to the discussion paper. If you have any questions please contact Brian Anderson, Senior Vice President, Technology Regulation at brian.anderson@bpi.com or (202) 289-4322.

Respectfully submitted,

Christopher Feeney
EVP and President, BITS
Bank Policy Institute

Annex A

The Bank Policy Institute (BPI) is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks. Its members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ nearly 2 million Americans, make 68% of all loans and nearly half of the nation's small business loans and serve as an engine for financial innovation and economic growth. The Business-Innovation-Technology-Security division (BITS) of BPI brings BPI's banks and other affiliate members together in an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector. For more information on BPI and BITS, visit http://www.bpi.com.