Martin Boer
Senior Director, Regulatory Affairs

August 22, 2023

Mr. John Schindler
Secretary General
Financial Stability Board (FSB)
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
(Submitted electronically)

Re: Third-Party Risk Management and Oversight

Dear Mr. Schindler:

The Institute of International Finance (IIF)[1] and its members are pleased to respond to the Financial Stability Board's (FSB) Consultative Document on "*Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*."[2]

This consultation builds on important work that the FSB has undertaken on regulatory and supervisory approaches to the management of outsourcing and third-party risk, including "*Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper*" (2020) and "*Third-party Dependencies in cloud services: Considerations on financial stability implications*" (2019).

The IIF has previously submitted its views in detail on these topics, including in response to the FSB's pre-consultation, "*Questionnaire on Third-Party Risk Management and Outsourcing*" in May 2022. The FSB's work also has a direct link to the IIF's work on cloud computing and financial innovation. In the IIF's view, financial institutions' migration to cloud service provision is a vital enabler of digital transformation and it promotes financial institutions' operational resilience.[3]

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.
[2] FSB 2023. "Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities" June 22, 2023.
[3] IIF 2021, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, January 8, 2021.

We appreciate the Industry Outreach Session that was conducted by the FSB on July 21, 2023, which provided excellent insights into the FSB's approach to this topic as well as a helpful discussion of industry views.

We are supportive of the FSB's long-standing leadership in promoting greater regulatory and supervisory harmonization, cooperation, and collaboration, which helps to reduce fragmentation in regulatory and supervisory approaches across jurisdictions and across the financial services sector. We encourage the FSB to continue its efforts to minimize regulatory fragmentation and we offer some suggestions for how these efforts could be advanced in the context of third-party risk oversight.

Overarching Comments

We are broadly supportive of the FSB's overall approach to third-party risk management. This letter will highlight some areas where the FSB could provide additional clarity on its approach, and we will provide some further considerations regarding third-party risk management from the financial services industry perspective for the FSB's consideration.

We also support the FSB's overall approach to the toolkit as a flexible instrument that is not intended to be interpreted as binding requirements. The FSB should further consider the need to balance regulatory interoperability with the flexibility of a toolkit that can be adapted to different legal and regulatory frameworks.[4] Further engagement among FSB members could be helpful in developing interoperable jurisdictional frameworks that reduce the negative impacts of market fragmentation, which makes the overall financial system more fragile and less resilient, efficient and secure.

We encourage the FSB to emphasize the concept of proportionality within the toolkit and in its discussions with FSB members. The final toolkit should recommend that FSB members conduct a careful balancing of costs and benefits and consider the negative impacts of detailed and prescriptive requirements on financial services innovation.[5]

The IIF supports the emphasis of the toolkit on *critical* third-party services. Given the FSB mandate to promote global financial stability, the emphasis of the toolkit should remain on service providers that support a financial institution's critical services. Services and service providers that are not critical generally have little or no potential to create financial stability concerns. That said, we are supportive of the consideration of non-critical service provider relationships where appropriate in relation to third-party registers and the management of concentration risks.

[4] The FSB could consider including in the toolkit language similar to that in the *Achieving Greater Convergence in Cyber Incident Reporting* paper that noted that financial authorities and financial institutions can choose to adopt the recommendations as appropriate and relevant, consistent with their legal and regulatory frameworks: https://www.fsb.org/wp-content/uploads/P130423-1.pdf

[5] One example of where a less prescriptive approach could be adopted relates to 'multi cloud' requirements that impose failover arrangements that may increase risks to financial institutions and increase cost and complexity, especially if the failover arrangements must be 'active-active.'

Definitions

Critical Service and Critical Third-Party Service Provider

We encourage the FSB to clarify the concept of critical services within the scope of the toolkit. In particular, we believe that the term 'critical service' should be revised to: (i) avoid potential confusion with respect to what this term intends to capture; and (ii) ensure an appropriate scope and criteria to identify third-party services which could significantly impair a financial institution's viability and impact broader system-wide financial stability. Other third-party services which do not meet these criteria should be out of scope.

Given this, critical services should be defined as those that would have a material impact on a financial institution's viability and a material impact on the financial stability of the financial services sector.

More generally, we encourage a clear and concise definition of critical services that would promote certainty for financial institutions, their regulators and supervisors, and third parties. To avoid any confusion, we recommend that the FSB update this term to 'critical third-party service,' defined as *'[a] service, the failure or disruption of which could significantly impair a financial institution's viability or critical operations.'*

It should be clear in the toolkit that a financial institution is responsible for determining whether a particular service is critical, regardless of whether the service is provided directly by the financial institution or the provision of the service is facilitated to a material extent by a third-party service provider.

A 'critical third-party service provider' should be defined as *a service provider that supports to a material extent the provision of critical services*.

This nuanced definition of 'critical third-party service provider' offers an important threshold for third-party service providers as there could be a number of ancillary third-party service providers that are supporting the provision of critical third-party services while not being essential to the delivery of those critical third-party services. It also recognizes that intra-group service providers should not include branches or business units of the financial institution, as these entities are under common control with the financial institution.

Systemic Third-party Dependency

We encourage the FSB to amend the definition of 'systemic third-party dependency' to focus on a dependency on one or more *critical* services, where disruption or failure may have systemic implications. A dependency on non-critical services should not have systemic implications.

Third-Party Service Relationship

The IIF encourages the FSB to modify the term 'third-party service relationship' to '*critical* third-party service relationship', in light of the importance of criticality in delineating the services and service providers that should be in scope of the toolkit. Further, the IIF recommends that the definition of a critical third-party service relationship explicitly acknowledge the need for a written contract. The written contract provides financial institutions with the legal authority to direct the critical third-party service provider to comply with the financial institution's third-party risk management processes and procedures.

The IIF's proposes the following definition of a 'third-party critical service relationship': *A formal arrangement for the provision of one or more critical services, or parts thereof, to a financial institution by a critical third-party service provider, pursuant to a written contract.*

Nth Party Service Provider

The toolkit should clarify that nth party service providers only include subcontractors (i.e. parties that are in privity of contract with the financial institution) that are clearly material to the provision of a critical service to the financial institution. Including nth party service providers that are not clearly material to the provision of a critical service to the financial institution could be overbroad and disproportionate to the risk that these nth parties could pose to the financial institution. Subcontractors should be expected to manage their own supply chain risks and are better equipped to do so than are the financial institutions to which they provide services.

We appreciate the FSB's acknowledgement that financial institutions rarely have automatic contractual relationships with these entities and, therefore, their ability to control those entities or to impose compliance requirements on them may be limited.

Intra-group Service Provider

Intra-group arrangements should be defined as those that involve the provision of critical services by a legal entity to another legal entity within the same financial group. Services that are provided by a branch or business unit of the same legal entity are not considered to be intra-group arrangements under established company law in most jurisdictions. A branch or business unit is generally subject to the governance, controls and operational arrangements of the legal entity of which is it a part.

Consistent with our definitional comments above, we encourage the FSB to update this term to 'intra-group third-party critical service provider.' The IIF proposes the following definition of an intra-group third-party critical service provider: *A service provider that is a legal entity under common ownership or control within the financial institution's group and that provides critical services to other legal entities within the same group.*

Other Definitional Issues

We request clarification as to whether the definitions of third-party service relationships and third-party service providers also include entities that provide products such as computer chips or other key components of information and communication technology (ICT) systems.

The toolkit notes that third-party service relationships exclude financial market infrastructure services, such as clearing and settlement, to other financial institutions. We encourage the FSB to extend the scope of this exclusion to third party providers already regulated by financial authorities.

Scope and General Approaches

We commend the toolkit's promotion of regulatory interoperability across jurisdictions and sectors (Section 2.3)

Promoting comparable, interoperable regulatory and supervisory approaches to third-party risk management can help address the challenges raised by market fragmentation, which makes the overall financial system more fragile and less resilient, efficient and secure. As the FSB notes,

having multiple, fundamentally divergent regulatory and supervisory approaches can create significant challenges to effective and efficient risk management of, and by, service providers that are subject to risks and threats that do not respect jurisdictional boundaries. Divergent regulatory and supervisory approaches can also increase financial institutions' administrative and compliance costs and regulatory and supervisory costs significantly without sufficient and proportionate benefits.

We encourage the FSB to promote the concept of home jurisdiction and group regulator/supervisor leadership with respect to the regulation and supervision of third-party risk management in order to better coordinate home and host country oversight and to avoid the negative effects of regulatory fragmentation on financial services groups. This is particularly valuable in light of the emergence of different jurisdictional approaches to the oversight of critical third-party service providers. Home jurisdiction leadership can result in significant efficiencies for both financial institutions and regulators and supervisors by, for example, reducing duplicative information requests or by requiring the same or substantially similar information to be produced in different formats or on different timetables.

Information sharing mechanisms can provide avenues to coordinate supervision and to discuss and address any host jurisdiction concerns about home country regulation and supervision. The FSB should consider adding language to the toolkit that would encourage regulators and supervisors to address any barriers to the sharing of information regarding their regulated or supervised financial institutions. The FSB should also encourage home and host regulators and supervisors to engage in joint exercises to assess the resilience of critical third-party service providers to the extent that their legal and regulatory frameworks provide them with the authority to conduct those exercises.

We strongly agree with the suggestion that was raised in the Industry Outreach Session to promote interoperable third-party registers with common data fields. Interoperable registers would mitigate considerably fragmentation risks for financial institutions and provide financial authorities with comparable data to help identify aggregate risk across the financial system and potential sources of systemic risk. The FSB should also encourage regulators to limit changes to the format of, and means and frequency of updates to, registers to those that are strictly necessary. This would help avoid the significant burden on financial institutions from changing requirements, which divert valuable resources from value-add risk management activities to more administrative tasks and manual updates to registers. We strongly encourage the FSB to establish a dedicated working group to pursue alignment of third-party registers, including the necessary data fields and data formats required to deliver information that meets common supervisory objectives.

We encourage the FSB to consider our comments below with respect to the impact of data localization requirements on regulatory interoperability.

We welcome the risk-based, proportionate approach to intra-group service relationships (Section 2.4). We believe that the concerns of regulators and supervisors outside of the jurisdiction of the intra-group service provider (noted in Section 4.4) could be addressed adequately through existing information sharing mechanisms.

The IIF appreciates the proportionate approach to third-party risk management of intra-group service relationships and recognizes that these relationships are not inherently risk-free.

Section 4.4 notes that financial authorities responsible for supervising the financial group's entities around the world may have less visibility of the critical services that those entities receive, the third-party service providers they receive them from, or the group's business continuity plans should these third-party service providers experience disruption or failure. The IIF believes that supervisory information sharing mechanisms provide a sound approach to addressing any such concerns. The group supervisor should liaise with the supervisor in the jurisdiction in which the intra-group service provider is located to provide host supervisors with appropriate and adequate information about the operations of the intra-group service provider and discuss concerns regarding that service provider.

Different treatment of intra-group services is justified because financial institutions generally subject intra-group services to well-controlled and globally consistent policies and processes. Given that intra-group services on a cross-border basis can reduce overall risk while improving efficiency, financial authorities should seek to encourage such arrangements and explore ways to enhance cross-border regulatory and supervisory efficiencies. This, for example, would enable a locally regulated legal entity to demonstrate that it is complying with the applicable local regulations and standards.

Financial institutions' critical third-party risk management

Considerations related to financial institutions' management of risks arising from critical third-party service provider concentrations

We appreciate the need for financial institutions to manage risks that may arise from concentrations in critical third-party service providers that are providing critical services to the financial institution. It is important for the FSB to note that a critical third-party service provider concentration at a financial institution can be mitigated with effective third-party risk management policies, processes and controls.

A financial institution is best placed to assess and manage the risks posed to its operational and financial viability by reliance on its own suppliers and critical third-party service providers. Financial institutions are responsible for identifying and managing concentrations risks resulting from their own usage of third-party services at the individual financial institution level as part of their overall risk management and employ a number of techniques and frameworks to manage third-party risks and concentrations. [6]

Financial institutions have long taken into account concentration risk (and other risks) related to their third-party service providers as part of their third-party enterprise risk management programs and have measures in place to both assess and mitigate these risks. Concentration risk is not new to financial institutions (e.g., risks associated with the use of financial market infrastructure) and has been managed effectively by the financial sector.

Individual financial institutions do not have the necessary oversight capacity to identify and monitor system-wide concentration risks. This is an area where financial authorities can contribute to greater system-wide stability, by monitoring concentration risks that exist across the broader financial industry.

[6] One such framework is the NIST Cybersecurity Framework, a new draft of which was recently released for public comment: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

Considerations related to financial authorities' monitoring of potential systemic implications of critical third-party service provider concentrations

The FSB and other financial services standard setting bodies could play a role in mapping concentrations at the global level that may give rise to systemic implications. This work could be modeled after similar work on central clearing interdependencies that the FSB has undertaken in the past with the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, and the International Organization of Securities Commissions. To this end, the FSB should engage closely with the other standard setting bodies and financial authorities to consider the interdependencies across the global financial system that may have implications for global financial stability and to establish common desired policy outcomes across sectors. Securing alignment on third-party register data fields, consistent with our response to Section 2.3 of the toolkit, is crucial to achieving this intended outcome.

Considerations related to the regulation of critical third-party service providers

Where consideration is being given to extending the perimeter of regulation to third-party arrangements in a particular jurisdiction, care needs to be taken to ensure that the burden of regulatory and supervisory requirements is proportionate to the risks posed by those arrangements.

The relationship between indirect regulation of third-party service providers and direct regulation of those service providers by financial regulators (or by proposed horizontal digital resilience regulators in some jurisdictions) should be clear whenever regulatory frameworks are articulated, and any cross-border implications should be carefully considered by the designers of those frameworks.

Onboarding and ongoing monitoring of service providers (Section 3.2)

We appreciate the need for robust due diligence, clear and legally binding contractual arrangements and ongoing monitoring and reporting from critical third-party service providers. While third-party service providers should be subject to robust operational resilience standards, it may not always be possible for financial institutions to negotiate the inclusion of these standards in service level agreements and related contracts. In certain areas, such as ensuring that a third-party service provider maintains robust business continuity plans, financial institutions are able to confirm compliance with the requirement but are unable to secure a more granular view due to the need to protect proprietary information. A better understanding of a third party's business continuity plans and how those plans would be executed – in particular, with respect to the business continuity plans of third parties deemed critical at the system level by financial authorities – could help financial institutions better calibrate their own plans. For this reason, we encourage financial authorities to facilitate closer participation and cooperation by third parties in joint industry exercises to allow for shared learning. The IIF believes that the FSB could also play an important role in encouraging financial authorities to promote these collaborative exercises.

The IIF agrees that pooled audits may be a possible source of assurance and information for both financial institutions and their regulators and supervisors. The usefulness of pooled audit and similar mechanisms is not confined to smaller, less complex financial institutions and the FSB is encouraged to promote these mechanisms to enhance the ongoing monitoring of service providers to financial institutions.

Incident reporting to financial institutions (Section 3.3)

Financial institutions' reporting to financial authorities on a timely basis is an important aspect of limiting third-party risk. The FSB should continue to encourage efforts among financial authorities to better align reporting conventions and thresholds in order to reduce regulatory fragmentation and streamline incident reporting processes for financial institutions.[7]

Management of risks from critical third-party service providers' supply chains (Section 3.5)

The IIF appreciates the recognition of the challenges of managing risks associated with critical third-party service providers' supply chains and fully supports the need for financial institutions to have a good understanding of critical third-party service provider key dependencies (i.e. those nth party service providers that are material to the provision of critical services) as part of their on-going due diligence and broader risk management programs. Financial institutions should focus their oversight activities on 'material subcontractors' in a supply chain supporting a critical service, where the disruption or failure of the material subcontractor could lead to an inability to provide the critical service.

Dedicating a financial institution's risk management to subcontractors that do not play a material role in the provision of a critical service would divert valuable resources from managing the most relevant risks of critical third-party arrangements. We support the FSB's focus on key nth parties and recommend that the final toolkit further clarifies that key nth parties mean subcontractors that provide a material part of a critical service, where the disruption or failure of the material subcontractor could negatively impact the provision of that critical service.

Section 3.5.4 indicates that financial institutions should create a risk rating of the critical third-party service provider's supply chain; we believe that this is overly prescriptive and duplicative to the risk rating of the critical third-party service provider. Supply chain risk management is already embedded in existing supplier and control assessments conducted by financial institutions. Ideally, certain contractual obligations, such as requirements for a third party to maintain a robust risk management program and to cascade contractual obligations to their subcontractors, could help to address supply chain risks. We strongly encourage the FSB to focus on the outcomes of third-party risk management, rather than prescribing specific methodologies which may be duplicative of existing practices or may not be suitable for all financial institutions' third-party risk management programs.

On a more granular level, it is not clear how this risk rating would be used and how this should (or should not) influence the overall risk rating that a financial institution already manages at the third-party level. Developing another separate risk rating of the components of the supply chain would duplicate the financial institution's risk management practices, given that the third-party risk rating (which includes supply chain risks) drives the controls required by the financial institution. We recommend that the FSB remove this concept and tool from the final toolkit.

We agree with the comments raised in the Industry Outreach Session that the FSB should consider further articulating the need for proportionality in the risk management of nth party relationships. While these relationships should be subject to appropriate risk management, the

[7] We support the FSB's Format for Incident Reporting Exchange (FIRE) as an example of reporting conventions and thresholds the promote convergence among cyber incident reporting frameworks.

requirements should not call upon the financial institution to duplicate the risk management processes and controls that have been established by the critical third-party service provider.

Exit strategies (Section 3.7)

The IIF appreciates the acknowledgement that there is no one-size-fits-all approach to exit planning. However, the IIF requests a clear differentiation and delineation between what is typically covered under Business Continuity / Disaster Recovery (BC/DR) plans and what is covered by exit strategies.

We believe that there is a time element that is important to highlight in discussing the interplay of exit strategies and BC/DR plans. In most cases (with the exception of sudden exits under stressed conditions), exit strategies do not play a role in BC/DR plans and exit strategies generally remain separate from broader BC/DR plans. BC/DR plans may need to be extended if the financial institution reaches a conclusion based on normal (and non-stressed) business considerations that it must exit a relationship with a third-party service provider over time. However, in more stressed scenarios (e.g. the bankruptcy of the third-party service provider) and/or where an alternative service provider must be arranged in a brief period of time, the exit strategy would become more of an integral part of the BC/DR plan.

The FSB notes, "[w]hile there are commonalities between different exit scenarios, exit strategies that are designed to be implemented over longer time periods may not be as useful to address significant disruption to critical services that cannot be remediated through other business continuity measures." The IIF believes that this point suggests that, if a financial institution is in crisis and cannot resolve the issues through its BC/DR plan, the financial institution should exit the third-party relationship. However, executing an exit plan may not be a preferred or an appropriate approach at a time of crisis as it may compromise the continuity of services by the financial institution or otherwise negatively impact the operational and financial viability of the financial institution.

Accordingly, the fourth bullet of Section 3.7 should be deleted, as pursuing an exit strategy during a period of extended disruption to critical services could substantially worsen the situation, to the detriment of customers and counterparties, and could have broader negative market implications.

Relatedly, in some cases, regulators may impose 'multi cloud' requirements on financial institutions, whereby critical services are subject to failover arrangements to another cloud service provider. Such prescriptive requirements may increase risks to firms and/or increase cost and complexity, particularly if the requirement impose failover installations to be 'active-active.' The U.S. Treasury noted in its whitepaper, *The Financial Services Sector's Adoption of Cloud Services*, that, "swapping complex workloads to another [cloud service provider] or bringing services in-house was often estimated to take months, if not years to successfully execute in almost all cases.[8]

Tools for financial authorities to identify and manage potential systemic risks (Section 4.3.4)

As noted above, the FSB should encourage sectoral financial authorities to conduct sector-wide and multi-sectoral exercises with respect to third-party service providers that may be considered

[8] https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

systemic. These exercises could be patterned after, and conceptually similar to, the supervisory stress tests of central counterparties. Exercises led by the sectoral standard setting bodies could help to pre-identify risks and help all market participants to better understand the actions they might need to take in response to those risks.

Other comments

Related comments on data localization

A significant impediment to regulatory interoperability (Section 2.3) is the imposition of data localization rules., i.e. rules which require data to be stored or processed locally,[9] which restrict the export of data, and impose costs on and hurdles to the innovation processes of internationally active financial institutions, without a commensurate increase in the achievement of regulatory objectives. Data localization rules create operational risk and can impede the provision of critical services by financial institutions, and the monitoring and mitigation of operational and other risks arising in connection with those services, by necessitating localization of the technology needed to manage or store data under local data management protocols that may not meet globally accepted standards. Data localization rules can restrict the provision of a range of services and innovations that are not commercially or technologically feasible under the data localization restrictions, to the detriment of customers and end-users. These rules can also result in more complexity and create additional attack surfaces that must be defended. Data localization rules have a detrimental impact on financial institutions' ability to fully leverage cloud solutions and can lead to complex IT architecture and duplication in systems setup, potentially creating new sources of information security risk.

The toolkit would benefit from further FSB guidance on how data localization requirements hinder the provision of critical services and can give rise to global financial stability concerns. One possible mechanism to address the barriers to the provision of critical services or effective risk management that are posed by data localization could be information sharing gateways that would allow the sharing by financial institutions of certain confidential information with trusted third parties, third-party service providers or supervisors.

Conclusion

We thank the FSB for its consideration of our comments and we would welcome additional stakeholder engagement around this topic in support of the FSB's goals of reducing fragmentation in regulatory and supervisory approaches, and thereby mitigating compliance costs and facilitating coordination among relevant stakeholders. If you have any questions or would like to discuss our comments in greater detail, please do not hesitate to contact Martin Boer at mboer@iif.com, Mary Frances Monroe at mmonroe@iif.com, Gloria Sanchez Soriano at gsanchezsoriano@iif.com or Laurence White at lwhite-advisor@iif.com.

[9] In our January 14, 2022 submission to the FSB on data frameworks affecting cross-border payments, we noted (at p. 2), these measures can take three broad forms: conditional limitations on data export (for example, on personal identifying information); local copy or processing requirements, i.e. the requirement to maintain a local copy of or process a particular data set in jurisdiction; or "hard" localization, i.e. outright prohibitions on data export, or where export is only permitted under very challenging conditions (such as individual regulator approvals).

Sincerely,

Martin Boer
Senior Director, Regulatory
Affairs Institute of International
Finance (IIF)