ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

**Andrew Ross**
Senior Vice-President
Payments & Digital

Tel (647) 730 4752
aross@cba.ca

August 22, 2023

Financial Stability Board (FSB)
Secretariat
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Delivered by email: fsb@fsb.org

## Re: CBA[1] Comments on FSB Toolkit for Enhancing Third-Party Risk Management and Oversight

The Canadian Bankers Association (CBA) welcomes the opportunity to share its response to the Financial Stability Board's (FSB) consultative document: *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities* (**the toolkit**). In addition to our comments below, we have provided more high-level responses in the attached Appendix.

The CBA lauds this effort by the FSB to develop a toolkit for financial institutions (FIs) and financial authorities that aims to reduce the risks posed by the disruption of critical services or service providers. We agree with the need for an international framework that strengthens the stability and resilience of the financial system and supports cross-border collaboration that reduces regulatory fragmentation across different jurisdictions.

Our prior submission[2] to the FSB recognized the challenges created by an environment defined by rapid change and increased levels of technological adoption. We continue to stress the importance of a holistic, technology-neutral, outcomes focused approach that allows banks the flexibility to manage risks related to third-party relationships in a manner that is proportionate to the risks posed.

In particular, we continue to caution against recommendations that would support prescriptive guidance which may stifle a FI's ability to innovate, adapt to the needs of a rapidly evolving technological landscape and to fully leverage the potential offered by third-party partnerships.

[1] The Canadian Bankers Association is the voice of more than 60 domestic and foreign FIs that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. www.cba.ca

[2] https://cba.ca/cba-comments-on-fsb-discussion-paper-on-regulatory-and-supervisory-issues

To minimize the operational complexity faced by financial institutions, the CBA believes that, wherever possible, any regulatory guidance should also leverage existing industry standards and recognized independent certifications that provide comparable or partial assurance to supervisors and ensure cross-border compatibility.

**Prioritizing Operational Resilience Without Sacrificing Flexibility:**

We agree with the holistic focus on third-party risk management that extends beyond outsourcing and focuses on risks in all third-party relationships. While we recognize that each FI will tailor their focus on operational resilience to the needs of their individual business, we emphasize the importance of alignment with available industry standards and consistency with current domestic regulations. Balancing flexibility and consistency in guidance is key to improving a bank's ability to identify, mitigate and monitor risks in a way that enables banks to prioritize their resources and focus on more critical services to ensure operational resiliency.

**Managing Critical Risks from Third-Party Relationships:**

We agree with the FSB that FIs are best placed to assess the criticality of services they receive, or plan to receive, from a third-party. If a FI determines that a relationship with a given third-party is material to a FI, it will then take the requisite steps to implement the appropriate controls that will enable the FI to monitor and manage any risks that may arise from the relationship or the supply chain of the service provider—in line with the principle of proportionality. Moreover, we reiterate the importance of providing flexibility for FIs in assessing the risk posed by different third parties to enable FIs to respond to challenges in an agile manner with minimum disruption to their operations.

**Cross-border Cooperation for Greater Consistency and Predictability:**

Differing regulations that result in regulatory fragmentation across multiple jurisdictions not only exacerbate the complexity around compliance but may also have a detrimental impact on banks' ability to manage risks across global operations in the event of conflicting requirements. Multiple jurisdictions, including Canada, are currently reviewing, or in the process of finalizing, their best practices around third-party risk management and we believe this might result in increased risk for potentially divergent or contradictory requirements.

For this reason, it is our view that the FSB can continue to play a role to support collaboration and coordination among domestic and international authorities to promote a harmonized approach towards global standards and reduce the risk of regulators issuing duplicative, conflicting, or unduly burdensome requirements for banks that operate across international borders.

Thank you for your consideration of our comments.

## Appendix

### Chapter 1: Common Terms & Definitions

**1. Are the definitions in the consultative document sufficiently clear and easily understood? Are there any important terms and definitions that should be included or amended?**

The common terms and definitions included in the toolkit are sufficiently clear and easily understood.

However, there are areas where additional clarity from the FSB would result in a more comprehensive toolkit. Additional guidance from the FSB would be welcome, for example, on the extent to which a third-party service contributes to the criticality of an FI's operations and how to differentiate between third parties that are directly critical to an FI's operations as opposed to those that contribute to other services that critical operations depend on or relate to at some degree.

We further note that the exclusion of Financial Market Infrastructure (FMIs) in the proposed definition for Third-Party Service Relationships does not align with recent and current practices in jurisdictions like Canada and the U.S. where regulatory guidance does include FMIs as third parties. It is also important to bear in mind that the definition of a third-party service does not remove the accountability a fourth- or fifth-party service provider in the supply chain has to manage its own risks.

### Chapter 2: Scope & General Approaches

**2. Are the scope and general approaches of the toolkit appropriate?**

We believe the scope and general approach adopted by the toolkit, with its focus on critical services, third-party oversight (as opposed to outsourcing), interoperability, and proportionality, is appropriate.

To provide additional clarity with regards to the scope and purpose of the toolkit, we suggest the FSB emphasize its role as a coordinating body across different jurisdictions and underscore the flexible, risk-based nature of the toolkit, which financial authorities and FIs may consider in accordance with their own circumstances, operating legal framework and the specific features of the financial services sector in their jurisdiction.

| Appendix |
| --- |
| Domestic regulators will subsequently be able to provide additional guidance around the applicability of any of these practices in the appropriate set of regulations, with respect to both practices required from the FI (section 3) and those approaches/tools applicable to regulators (section 4). |
| **3. Is the toolkit's focus on regulatory interoperability appropriate? Are there existing or potential issues of regulatory fragmentation that should be particularly addressed?** |
| The toolkit's focus on regulatory interoperability is appropriate and relevant. Regulatory fragmentation, particularly in the context of overlapping requirements by different financial authorities, may result in regulatory redundancy, inconsistency, and inefficiency. While regulatory homogeneity is an impractical objective given the varying legal systems involved, greater coordination between regulators and FIs can contribute to more harmonized regulatory regimes that do not impose inconsistent requirements on FIs.<br><br>Accordingly, we believe the FSB should also consider including in the toolkit additional guidance or recommendations for financial authorities and regulators on how to manage FIs that are subject to multiple regulators across different jurisdictions, particularly in areas where requirements or approaches could be perceived as contradictory.<br><br>Clarity on regulatory flexibility is particularly important for FIs with operations in more than one country and may reduce the regulatory burden of maintaining more than one third-party risk management framework to satisfy multiple regulations across different jurisdictions. Moreover, as the FSB notes, we agree this work could not only help mitigate compliance costs for FIs, but for third-party service providers as well. |
| **4. Is the discussion on proportionality clear?** |
| Greater clarity on the criteria of proportionality, which are outlined but not defined, would also be welcome. For example, while a FI's size is listed as a criterion for consideration, it is unclear what constitutes a "large" or "small" FI when determining proportionality. |
| **Chapter 3: Financial Institutions' Third-Party Risk Management** |
| **5. Is the focus on critical services and critical service providers appropriate and useful? Does the toolkit provide sufficient tools for financial institutions to** |

| Appendix |
| --- |
| **identify critical services? Do these tools rightly balance consistency and flexibility?** |
| While the toolkit's focus on critical services is useful and appropriate, allowing, for example, for the identification of critical services based on substitutability, operational or strategic importance or the impact of a service disruption, the toolkit would benefit from additional tools that focus on other types of services that are not necessarily critical. The toolkit's extensive focus on "critical services" can also benefit from being complimented with additional guidance or best practices to support FIs in the identification and management of critical service providers as well as the relationship between critical services and critical service providers.<br><br>As we note in our first answer, the toolkit does not provide sufficient clarity on which specific services and relationships are actually 'critical' from the perspective of an individual FI as opposed to those that are critical to the stability of the whole financial system.<br><br>However, we believe the tools strike an appropriate balance between consistency and flexibility given their framing as considerations, not requirements. There is also interest in evaluating the FSB's proposition to include an assessment of potential benefits and risks related to the provision of critical services from service providers. |
| **6. Are there any tools that financial institutions could use in their onboarding and ongoing monitoring of service providers that have not been considered? Are there specific examples of useful practices that should be included in the toolkit?** |
| While Chapter 3 references the third-party lifecycle – Planning, Due Diligence, Contracting, Ongoing Monitoring, and Termination, the toolkit lacks a section on Planning (i.e.: Assessment of Inherent Risk), as it appears to merge initial due diligence and inherent risk assessment into a single step. |
| **7. What are the potential merits, challenges and practical feasibility of greater harmonisation of the data in financial institutions' registers of third-party service relationships?** |
| Greater harmonization in third-party service registries will provide a clear benefit by supporting the ability to identify concentration related risks by systemically important third parties. Some key challenges include the consistent mapping of third-party service relationships in the absence of a consistent service or risk taxonomy (particularly in a cross-border context). Other challenges include a limited ability, in general, to identify and/or validate $n^{th}$ parties, and supply chain dependencies, particularly in circumstances where little leverage is available to enforce the provision of supply chain information by a third-party. In |

| Appendix |
| --- |
| some situations, FIs simply may not have the resources required to ensure that a given third party provides information regarding their supply chain. |
| **8. Are the tools appropriate and proportionate to manage supply chain risks? Are there any other actionable, effective, and proportionate tools based on best practices that financial institutions could leverage? Are there any other challenges not identified in the toolkit?** |
| We generally agree that the risk-based approach adopted by the toolkit and the tools provided are appropriate in the context of managing supply chain risks. We believe the focus of the toolkit should be on those relationships considered critical to assess whether the supply chain is a key factor to be managed (where identified as a risk on a case-by-case basis). The toolkit should also aim to clarify the expectations around third-party services that are not necessarily critical but may support critical services to some degree (individually or along with other services). We also agree with the limitations outlined such as gaps in the information provided by a third-party and the resources required to identify and monitor risks related to $n^{th}$ parties.<br><br>It is, in general, important to also bear in mind the added levels of complexity to and resources required by individual FIs that are created by proposals to mitigate supply chain risk, such as increasing the number of risk assessments to cover the entire or a significant part of the service provider's supply chain. Such proposals could result in the diversion of resources to lower risk/less critical services, which might potentially impact an FI's ability to manage risks in manner that promotes operational resilience both within the FI as well as the broader financial system.<br><br>We also recognize that challenges remain in developing an effective set of practices to mitigate supply chain related risks. For example, it may not be feasible in many cases to determine a risk rating for the supply chain of a critical service provider for the reasons we note above.<br><br>The toolkit could also provide additional guidance on how to address the disparity in bargaining power that may exist (that favours the third-party) and how to manage confidentiality rights between the third-party and their providers (i.e. $n^{th}$ parties) and related tools to support FIs in their assessment of risks posed by a third-party and their provider.<br><br>Regulators should assess the wide range of tools at their disposal as they aim to address the limitations surrounding a FI's management of supply chain risks beyond its direct third-party, particularly those that affect the providers of critical services to FIs or critical suppliers to the financial system whose disruption can cause considerable systemic consequences. This is particularly important in circumstances where an FI cannot enforce their own rules in a relationship with a third-party that is relied on and cannot be replaced. |

| Appendix |
| --- |
| Hence, regulation at the level of $n^{th}$ parties should be assessed for its feasibility and impact on FIs as any discretional requirements will increase the cost of the supply chain which will ultimately impact the FIs, clients and financial system overall. |
| **9. What do effective business continuity plans for critical services look like? Are there any best practices in the development and testing of these plans that could be included as tools? Are there any additional challenges or barriers not covered in the toolkit?** |
| We believe that effective business continuity plans for critical services are appropriately detailed in section 3.6.3.<br><br>However, it is worth noting that effective business continuity plans will vary by organization but should ultimately align to industry standards. We also note a lack of consistency between FSB guidance and related domestic guidance, with regards to exit planning, and it is important to recognize that the lack of a feasible exit plan constitutes a risk itself that an FI must manage. Given the difficulties in exiting certain arrangements and limited awareness of related risks, there is limited recourse for a feasible exit plan in certain circumstances.<br><br>We believe that annual Disaster Recovery (DR) testing for suppliers that are identified as providing critical technology services aligns with current best practices. The intent of testing the plans is to ensure that interdependent processes can successfully demonstrate resilience and to mitigate the potential for a third-party incident to impact critical products or services.<br><br>One additional consideration is to have language on business continuity management plans incorporated into contracts with vendors to ensure the appropriate documentation can be reviewed. This can serve to mitigate the risk of a supplier being unable to recover during a major incident or disruption. The contract language may also drive the need to conduct integrated testing with critical suppliers on a periodic basis. If the contract language is not included, then it may present more challenges for FIs to obtain the required evidence for a business continuity plan. Regulators could also consider how to support FIs in mitigating risks emerging from business continuity planning, particularly in circumstances involving a critical supplier or service whose disruption poses systemic consequences. |
| **10. How can financial institutions effectively identify and manage concentration and related risks at the individual institution level? Are there any additional tools or effective practices that the toolkit could consider?** |
| We believe it is important to recognize there may be challenges and risks that could arise as a result of the concentration of third-party service providers; however, we caution against overly prescriptive mitigants that may risk increased operational complexity, which would contribute to additional operational and systemic risks that would ultimately be counter to regulators' policy intent of ensuring operational resilience. Banks also undertake risk-based |

| Appendix |
| --- |
| approaches to managing the risks associated with third-party relationships if the substitutability of a service is not tenable.<br><br>A potential tool for identifying third-party concentration risk at the FI level is keeping up-to-date third-party libraries with relevant data points (ie., Geography, Service Provided, Key 4th / nth parties, etc.). This data would drive concentration risk reporting, with enterprise-wide tolerances in-place. |
| **11. Are there practical issues with financial institutions' third-party risk management that have not been fully considered?** |
| The regulatory burden of increased requirements/guidelines must be considered, as well as the limitations of assessing and managing nth party risk (due to factors such as audit rights, supplier refusal, gaps in third party service provider transparency, etc.). |
| **Chapter 4: Financial Institutions' Oversight of Third-Party Risks** |
| **12. Is the concept of "systemic third-party dependencies" readily understood? Is the scope of this term appropriate or should it be amended?** |
| Our view is that the concept of "systemic third-party dependency" can benefit from additional clarity, particularly to support an individual FI's determination of which third parties are, or are not, considered systemically important third-party service providers. Any service from any third-party supporting a non-critical process can be linked to other services or processes that would eventually, alone or with other services, rollup into a critical operation.<br><br>While this provides flexibility to the FIs to define what is relevant for their situation, some minimum criteria and considerations could be suggested to ensure regulators do not have unreasonable expectations around the evaluation and treatment of the FI's supply chain beyond third parties and most relevant nth parties.<br><br>We also believe that most FMIs provide services that FIs require to perform the "bare minimum" functions needed to effectively operate and therefore they would ultimately be considered systemically important. It is also important to note the difficulties that emerge from the treatment of (currently) non-regulated entities that are considered systemically important. |
| **13. How can proportionality be achieved with financial authorities' identification of systemic third-party dependencies?** |
| It is challenging to achieve proportionality in the financial authorities' identification of systemic third-party dependencies. It is our view that proportionality, size, and relevance of the FI |

| Appendix |
| --- |
| should be considered when designating systemic third-party dependencies. Exceptions to the requirements of the treatment of systemic third parties should be considered based on criteria such as the size of the FI, exposure, amount of dependency on the third-party service provider, etc.<br><br>Regulators also need to understand that their active role in identifying systemic dependencies through an approach that solely relies on FIs to do so is insufficient. While FIs can play a significant role in managing systemic risk through their practices, disclosing data for risk management purposes amongst FIs has positive effects up to certain extent and could raise concerns related to competition if the obligation for information exchange was unreasonable.<br><br>Regulators have additional tools at a lower cost that can be used to the benefit of the financial system, including data from all financial actors under their purview and a holistic, integrated view of these actors at a major scale beyond the risk of an organization.<br><br>Additionally, regulators can consider how to leverage tools to encourage collaboration from service providers in situations where support from FIs is not feasible. Regulators are also encouraged to share their findings related to systemic concentration risk with FIs in support of a collaborative approach to mitigating third-party risk. |
| **14. Are there any thoughts on financial authorities' identification/designation of service providers as critical from a financial stability perspective?** |
| We emphasize the desirability of having FIs retain a degree of flexibility to individually assess the criticality of their service providers while also ensuring that individual FI perspectives inform the views of financial regulators if they are undertaking a role to designate service providers as critical.<br><br>High levels of cooperation between service providers and FIs still does not eliminate the need for an entity with a holistic view of the financial system to identify and assess criticality and concentration risk. However, we caution against the risk of mischaracterizing what services are critical if the responsibility for the designation falls squarely in the hands of a national regulator.<br><br>Ultimately, if a regulator is contemplating this as an option, we believe consultation with industry is needed as any criteria that is developed to support the identification or designation of critical service providers must be clear, measurable, regularly reviewed, and consulted upon by FIs. As mentioned above, financial institutions' treatment of service providers deemed "critical" should be proportionate to the FI's exposure, size, etc. |

| Appendix |
| --- |
| **15. Should direct reporting of incidents by third-party service providers within systemic third-party dependencies to financial authorities be considered? If so, what potential forms could this reporting take?** |
| We believe FIs are the right stakeholders to understand the implications of an incident that relates to the services they receive and should be the contact of regulators in these situations.<br><br>Our view, considering the relationship in question is between the FI and their third-party service provider, is that regulators should obtain access to information relating to incidents of this kind from the FIs rather than from the providers themselves.<br><br>Regulators can require additional information from FIs, if needed, and under clear and exceptional circumstances (e.g., when there is a systemic impact on the financial system) regulators can then, as a last resort, and in the context of their own legal and regulatory framework, explore the feasibility of enforcing exceptional measures including direct monitoring on third parties providing critical services.<br><br>Furthermore, during significant incidents, resources both at the third-party and the impacted financial institutions would likely be allocated to remediation efforts. Depending on the expected notification timelines, reporting to financial authorities may cause potential delays to the remediation process.<br><br>A different approach could bring unwanted consequences to the FIs and system overall, including legal risks for the FIs, transaction costs around the contracting process to enable these requirements, increasing costs of services or need for insurance, etc. – which could increase the overall cost of using the financial system.<br><br>Additional considerations include:<br><br>- Is there potential that systemic third-party service providers would not comply?<br>- What actions would financial authorities be expected to take?<br>- How would financial authorities use this reporting data? |
| **16. What are the challenges and barriers to effective cross-border cooperation and information sharing among financial authorities? How do these challenges impact financial institutions or service providers?** |
| We believe a key challenge to effective cross-border cooperation is the differing set of criteria for what constitutes a “systemic third-party dependency” and third-party service provider when determining the criticality of a third-party in terms of the impact its disruption will have on the stability of the financial sector. |

| Appendix |
| --- |
| The criteria would likely be informed by the FIs within their respective jurisdictions and would likely differ due to different jurisdictional risk exposures, size, and maturity. An improper set of criteria for identifying systemic third-party dependencies may result in inappropriate risk management requirements. Differing legal rights of financial authorities amongst jurisdictions may further impact the cooperation/coordination of regulatory action.<br><br>Three other key challenges include:<br><br>- Differing financial authorities' mandates, frameworks, legal requirements, power over third-party service providers, etc.<br>- Practical challenges of coordinating supervisory activities across different jurisdictions.<br>- Challenges in sharing sensitive information.<br><br>To address these challenges, it is our view that regulators consider formal collaboration (made known to FIs) driven by common frameworks that cover the rules and expectations around cross-border collaboration. Effective cross-border cooperation can create lower costs for FIs and generate additional efficiencies in the regulatory review process and ultimately enhance the resilience of FIs operating in multiple jurisdictions. |
| **17. Are there any views on (i) cross border information sharing among financial authorities on the areas covered in this toolkit (ii) including [certain third-party service providers] in cross-border resilience testing and exercises, including participation in pooled audits?** |
| It is important to bear in mind concerns related to the sharing of sensitive information in the context of cross-border information sharing and to clarify where the proper consent of a third-party is required in light of a given FI's legal obligations. To mitigate these risks, regulators and international standard setters like the FSB should encourage alignment on a common framework for collaboration purposes that is mindful of these considerations. |
| **18. Are there specific forms of cross-border cooperation that financial authorities should consider to address the challenges faced by financial institutions or service providers?** |
| No additional comments here. Please refer to responses to questions 16 and 17. |