Date: August 21, 2023

From: Andrew Moyad, CEO, Shared Assessments LLC

To: Financial Stability Board, fsb@fsb.org

Subject: Third-Party Risk Management and Oversight

RE: Third-Party Risk Management and Oversight—FSB: June 2023 Consultative Document—Enhancing Third-Party Risk Management and Oversight Shared Assessments Program Regulatory Response

Shared Assessments LLC appreciates the opportunity to submit comments to the Financial Stability Board.

Shared Assessments has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body that defines best practices, develops tools, and conducts leading research. Program members are public and private organizations that work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy, and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

On behalf of our organization and its members, thank you for accepting the following response in regard to the FSB's June 2023 Consultative Document—Enhancing Third-Party Risk Management and Oversight.

--**

Shared Assessments believes that the toolkit's three fundamental objectives are entirely appropriate:

- To reduce fragmentation in regulatory and supervisory approaches to financial institutions' third-party risk management across jurisdictions and different areas of the financial services sector;
- To strengthen financial institutions' ability to manage third-party risks and financial authorities' ability to monitor and strengthen the resilience of the financial system;
- To facilitate coordination among relevant stakeholders (i.e., financial authorities, financial institutions and third-party service providers).

We suggest the FSB carefully consider how toolkit recommendations might generate incremental compliance costs to both financial institutions and third-party service providers and how those costs might be mitigated.

Chapter 1

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?

Partially. The FSB definitions as written are generally clear. The following definitions bear discussion.

- ***Interoperability:*** The term "interoperability" is defined within the narrative as: "*difference both between jurisdictions and regions, and across different areas of the financial services sector. Consequently, regulatory and supervisory interoperability in the context of the toolkit seeks to ensure that individual regulatory and supervisory regimes do not lead to inconsistent requirements and expectations on financial institutions and service providers operating internationally. It does so by setting out aligned and comparable, outcomes-based frameworks to manage third-party risks, while avoiding a one-size-fits-all approach that does not permit differences in regulation or market structure. Pg. 9-10, FSB."*

  Regulatory interoperability may be easier to achieve in some—but not all areas (e.g., regulatory requirements may be easier to align with the guidance versus actual exam standards, and an appropriate cyber standard of care versus the complexity of harmonizing multiple international privacy frameworks). A workable approach built around incremental steps to identify where harmonization can be achieved with less friction could be a foundation for an effort to close policy gaps in the longer term.

- ***Outsourcing****: A category of third-party service relationships where a financial institution uses a service provider to perform, on a recurrent or an ongoing basis, services, or parts thereof, <u>that would otherwise be undertaken, or could reasonably be undertaken, by the financial institution itself</u>.*

  The proposed definition is reasonably clear. However, the definition could acknowledge that not all outsourcing results from activities that could reasonably be undertaken by a financial institution. In today's rapidly evolving technology landscape characterized by rapid innovation, many FIs utilize third parties to deliver services that they themselves are not equipped to deliver. US regulators have recently established adjunct regulatory programs, such as the Novel Activities Supervisory Program, that are designed to enhance current regulatory supervision in areas where FIs work with partners to deliver complex emerging products and services where the novel manifestation of associated risks is not sufficiently clear. Accordingly, we suggest that expanding the definition to recognize that

third party performance of many necessary operational functions or services could enhance the service delivery, control standard of care, or both. For example, an additional point to this definition could read as follows: "However, where a financial institution would not reasonably be expected to have the requisite skills, competence, licensing requirements, or experience in other forms of business activity (e.g., architectural/engineering design, construction, data center management, healthcare, specialist consulting or legal services), the use of third parties would not constitute an outsourcing per se but still require appropriate diligence and oversight based on the criticality and risks involved." Modifying the definition by removing "…*that would otherwise be undertaken, or could reasonably be undertaken, by the financial institution itself*" *would make it more accurate.*

- ***Critical service****: A service whose failure or disruption could significantly impair a financial institution's viability, critical operations, 2 or its ability to meet key legal and regulatory obligations.*

  The FSB definition of critical service omits any mention of customer impact, which should be explicitly acknowledged in updated language. The FSB should consider this revised definition: *A service whose failure or disruption could significantly impair a financial institution's viability, critical operations, key customer obligations, or its ability to meet key legal and regulatory obligations. "…key customer obligations,…" is the recommended addition.*

- ***Systemic third-party dependency****: A dependency on one or more services provided by a service provider to financial institutions where their disruption or failure has been identified by a relevant financial authority as having potential implications for financial stability.*

  The definition of systemic third-party dependency is clear and understandable. Systemic third-party dependencies should always be determined by Financial Authorities; individual financial institutions lack the visibility to make reliable designations. However, the following modifications would clarify a risk-based focus on materiality: "A dependency on one or more services provided by a service provider to financial institutions where their disruption or failure has been identified by a relevant financial authority as having *potentially significant* implications for *either short-term or long-term marketplace* financial stability."

  The FSB should consider the addition of an additional term, *Critical Third-Party Supply Chains.* The definition could acknowledge the reality that a failure in supply chains with multiple critical service providers (or service providers that on their own might not be critical but in combination present sufficiently heightened risks to earn a critical designation) could have an outsized impact on financial institutions. When there are multiple dominant (but not necessarily critical) providers in a supply chain sector, the definition does not address this potentially cascading impact. Alternatively, this could simply represent an added consideration in determining any systemic third-party dependency (i.e., whether stemming from a single third party or multiple third-party dependencies that are linked).

Chapter 2

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

Yes. The scope and approaches are appropriate. The toolkit's focus on proportionality, critical services, and critical third parties that have the potential to cause material disruption to the financial services sector (systemic third-party dependencies) are particularly useful.

3. Is the toolkit's focus on regulatory interoperability appropriate? Are there existing or potential issues of regulatory fragmentation that should be particularly addressed.

Yes. The toolkit's focus on regulatory interoperability is overdue. The specific expectation for greater regulatory harmonization is reasonable and important to avoid ongoing mismatches and inefficiencies in many regulated entity control programs.

This language is particularly helpful: *It is important to note that interoperability does not mean homogeneity. Complete regulatory and supervisory alignment is unlikely to be possible or practical, given legal differences between regimes and the different business models of financial institutions, which mean that risks can differ both between jurisdictions and regions, and across different areas of the financial services sector.*

Consequently, regulatory and supervisory interoperability in the context of the toolkit seeks to ensure that individual regulatory and supervisory regimes do [do not result] not lead to inconsistent requirements and expectations on financial institutions and service providers operating internationally.

However, regulatory interoperability may be easier to achieve in some areas than in others. A workable approach built around incremental steps to identify where harmonization can be achieved with less friction could be a foundation for an effort to close policy gaps in the longer term.

4. Is the discussion on proportionality clear?

Yes. Proportionality, the realization that "*The failure or disruption of a critical service may have a greater impact on financial stability if it affects larger, more complex financial institutions"* is widely recognized by regulators internationally. The FSB's recognition and discussion around the significance of the concept of proportionality supports rational allocation of resources to the extent that the outsourcer understands the residual risk associated with its riskiest suppliers/services and then applies the most effective resource intervention to mitigate those risks.

Chapter 3

5. Is the focus on critical services and critical service providers appropriate and useful? Does the toolkit provides [sic] sufficient tools for financial institutions to identify critical services? Do these tools rightly balance consistency and flexibility?

Partially. While the toolkit notes that a common framework for the identification and management of critical services can provide consistency and comparability, the toolkit can also facilitate the identification of systemic third-party dependencies by financial authorities, which is very important for both outsourcers and third-party providers. Regulators across the globe have increasingly focused on critical third parties and services for good reason. Critical suppliers can have an outsized impact if their services are interrupted. Critical suppliers also require increased organizational resources to ensure they meet contractual expectations and meet the challenges associated with rapidly changing risk environments.

Focus on substitutability is very important, as FIs operate in some environments where rapid substitution or service transfers are impractical or impossible. Financial Authorities should base critical third-party designation on the role those parties play in supporting the critical services that financial sector firms provide. This consideration is required under the UK Prudential Regulatory Authority

Operational Resilience DP3/22; while this requirement is not present in the United States, the increasingly complex sourcing chain, as noted by the Financial Stability Board, mandates a deeper understanding of the chain's full extent. While there are very specific rules (e.g. GDPR, DORA), multiple pieces of legislation are mandating guidance, and these disparate rule sets often create more problems than a clear, consistent direction or point towards appropriate, workable solutions.

Discussion of how the criticality of services can change over time is useful, and the specific examples cited (corporate reorganizations and mergers) are often overlooked. The FSB accurately emphasizes proportionality again in this reference: *Financial institutions can assess the criticality of a service prior to entering into a third-party service relationship and reassess it regularly during scheduled review periods, when planning to change their use of the service, and when there is a material change to the service or the service provider (e.g. a corporate reorganisation or transaction, such as merger, that may impact the provision of the relevant service). FSB, pg. 12.*

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?

Yes. Notably, the items detailed in the FSB's Section 3.2.1. (pgs. 13-14) of the Consultative Document are comprehensive and appropriate. Management of supply chain risks is a welcome addition.

However, in practice there is a greater gap in the planning, RFP, vendor selection, and onboarding stages than in other areas of due diligence. Time pressures to introduce or improve a service may limit an institution's practical ability to "ideally" assess a third party during the vendor selection process. The toolkit could consider speaking to that situation specifically. Current practice is not sufficiently stringent around contractually ensuring that the provider can meet (or exceed) the outsourcer's hygiene nor ensure an appropriate level of hygiene is maintained throughout the vendor lifecycle.

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?

Without current, complete, and accurate critical third-party information, regulators and FIs cannot accurately determine critical systemic third-party dependencies. For that reason alone, standardized register harmonization is an important goal. For critical third parties, standardized registers should include third and N^{th} parties including a criticality designation based on common criteria and clear, concise guidance – documented by the regulator – depicting when N^{th} parties should be included in those registers.

It is vital that consistent regulations across jurisdictions on N^{th} parties register inclusion is both present and widely understood. Existing US guidance under recent consolidated FRB/FDIC/OCC Interagency Guidance mandates current inventories of all third-party relationships (and, as appropriate to the risk presented, related subcontractors). Critical activities, vendors, and N^{th} parties should be designated in registers. Because financial authority use of registers is inconsistent across jurisdictions, regulators should clarify and consistently communicate the intent and purpose of guidance around third party registers.

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?

The consultative document accurately notes that *"it can be impractical for each financial institution to directly assess and manage every unique risk across each element of their third-party service providers' supply chains. There are practical limitations to financial institutions' ability to directly monitor and manage these risks."* It goes on to suggest that when evaluating supply chains *"the toolkit should be applied in a proportionate and risk-based manner. This means that the toolkit does not necessarily cover all nth-party service providers in third-party service providers' supply chain."*

Therefore, we believe that FI supply chain evaluations should be focused on situations where a critical N^{th} party service provider has been identified or where a financial institution has identified a degree of outsourcing chain complexity that it believes might reasonably cause a material issue.

Financial institutions have had a degree of success using N^{th} party continuous monitoring techniques, data often supplied as a feature of a monitoring service, to develop greater insight into their supply chain structure. However, even when those data are provided, FIs must spend considerable effort to confirm the materiality of specific downstream relationships. This work is exceedingly difficult, and sometimes impossible for all but the largest FIs, to scale this discovery process.

9. What do <u>effective</u> 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?

There is an essential difference between effective business continuity plans for a single company (whether an FI or their third parties) from effective ones for critical services. Namely, an effective business continuity plan (BCP) for critical services requires plans that are mutually developed and agreed upon by an FI and their relevant third party(ies) associated with a critical service. This requires a completely different approach and higher degrees of communication and cooperation between firms than a conventional BCP normally entails. Unless there are either contractual obligations or operational artifacts that specify how an FI and their relevant critical service providers will actually declare, communicate, and mutually address critical service failures, any form of BCP plan will remain incomplete and provide false comfort. Best practices in the development of such plans include a defined cadence for combined plan updates and testing, mechanisms for mutual remediation planning, and defined key performance indicators (KPIs) and key risk indicators (KRIs) associated with such plans to signal potential gaps or weaknesses between plan review periods that involve either party. These represent gaps in the toolkit, which takes the more conventional approach of focusing on each party's BCP in isolation. The information remains useful, and the toolkit does highlight the need for joint testing, but this could go further by promoting these additional points to promote greater alignment and direct collaboration between an FI and their critical service providers in their planning and testing.

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?

The Consultative Document's text identifies three considerations when defining concentration risk:

- *The overall number of services supported by a single or closely connected service providers;*
- *The number of critical services supported by a single or closely connected service providers (sometimes referred to as "aggregation"); and/or*
- *Exposure to certain jurisdictions or regions.*

Managing supplier concentration is often a balancing act between minimizing a firm's exposures to an excess of third parties, achieving operational resilience and benefiting from efficiencies that emerge when a single supplier supports multiple outsourced activities. The presence of critical suppliers demands incremental risk management processes from the outsourcer. A priority is often identifying and planning for the substitution of critical third parties. Substantial substitution issues can occur when there is a lack of real alternatives, high switching costs, and complicated migration logistics. Issues such as these should be identified early and communicated to regulators.

At the individual institutional level, where needed, FI firms should elevate their standard of care by identifying and managing concentration and related risks using the latest tools for deeper analysis. In particular, very common, legacy practice involves the mere compilation of supplier lists and their periodic review. While this represents a useful start, such data cannot provide meaningful strategic insights, while process mapping, supply chain diagrams, and other dynamic tools to highlight the risks and resilience of a firm's third-party ecosystem are more essential today. Too often, firms have far stronger insights about their competitive landscape than their supplier landscape. As a result, this needs attention for both resilience and competitive reasons to ensure FI firms have real-time intelligence about their dynamic concentration risks, whether due to limited supplier numbers, their service locations, or even limited resilience across a range of services/N^{th} parties.

In environments where regulators have determined that a supplier has been designated as a systemically-important entity, that information should be routinely disclosed by the regulator to interested parties.

11. Are there practical issues with financial institutions' third-party risk management that have not been fully considered?

Yes. A commonly overlooked point about risk management is that many third parties often provide superior services, stronger working control frameworks—or both—relative to an FI. As a result, both inherent and residual risk assessments associated with critical services need to consider the collective impact to an FI firm's exposures by engaging a third party, not merely how much more or less exposure that third party may introduce on its own. Related, however, where a third party may contribute superior products or services beyond the standard experience or expertise of an FI firm, the ability of the FI firm and its managers to evaluate and effectively oversee such third parties may be challenged or even impractical, which demands an ongoing need to ensure independent parties of experts routinely audit or assess those critical third parties and review those results and their implications in a meaningful way with FI firms.

Chapter 4

12. Is the concept of "systemic third-party dependencies" readily understood? Is the scope of this term appropriate or should it be amended?

Yes, this is readily understood, and the scope of this term is appropriate. Financial Authorities are the only current entities with sufficient cross-market visibility to identify systemic third-party relationships. We agree that DORA, specifically Article 28, is a valid model for this purpose, as referenced in FSB Annex A. However, what is not readily understood at this early stage and what will invariably create uncertainty is the detailed nature and degree of data collection that the Financial Authorities will either propose or expect. This warrants more industry feedback as these ideas develop. For now, the items proposed within the Consultative Document are all appropriate, and the noted challenges of the related

data collection are well considered, including the concern about not hampering real-time remediation efforts during major events.

13. How can proportionality be achieved with financial authorities' identification of systemic third party dependencies?

By providing guidance that leverages the Financial Authorities' ability to identify and designate a systemic third party dependency to determine when there could be differential impacts within the sector based on the size/reach of the FIs affected. This incremental guidance would improve the ability to achieve proportionality. This analysis should be based on whether the failure of that third party results in a wholesale disruption of activities within the sector. Therefore, there should not be a one-size-fits-all approach.

In some jurisdictions regulators are, or are planning to, assume greater third party oversight responsibility on behalf of smaller financial institutions. A Federal Reserve Board member recently noted that "The third-party service provider landscape has continued to evolve and expand. As a result, we should consider the appropriateness of shifting the regulatory burden from community banks to more efficiently focus directly on service providers. The Bank Service Company Act gives the federal banking agencies significant regulatory authority over outsourced banking services. In a world where third parties are providing far more of these services, it seems to me that these providers should bear more responsibility to ensure the outsourced activities are performed in a safe and sound manner." (Welcoming Remarks, Michelle W. Bowman, Member, Board of Governors of the Federal Reserve System at Midwest Cyber Workshop, Organized by the Federal Reserve Banks of Chicago, Kansas City, and St. Louis, February 15, 2023). The logical consequence of these remarks is that regulatory authorities must have a closer supervisory purview regarding third parties, especially those they have designated as critical. Such a level of authority is necessary to identify and resolve issues for third party dependencies with sector-wide impacts that any one small financial institution may not detect or even have the resources to address legally or operationally.

14. Are there any thoughts on financial authorities' identification/designation of service providers as critical from a financial stability perspective?

Yes. Regulators should examine the concentration characteristics (for example, how easy is substitutability) as well as the specific services the party supports, as those characteristics would be the most salient in the Financial Authorities' criticality evaluation.

Beyond that response, the full intention of the question is not clear. The question can be read either as the financial stability of the third party, or the financial stability of the sector. The implication of the question is that under a given set of circumstances a service provider may fail as a function of financial stability causing industry wide consequences. It is not clear that the reason for failure is material – rather, it is the *impact* of failure (or possible failure) that is relevant. The other reading of this question is whether only the financial stability of the sector is at risk. This perspective would be the basis for making the determination of when a service, by definition, is critical.

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?

Yes. Notably, current U.S. regulations require that bank service providers *"notify each affected banking organization customer as soon as possible when the bank service provider determines it has experienced*

a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours." Banking organizations are then required *"to promptly notify [their] primary Federal regulator of any ''computer-security incident'' that rises to the level of a ''notification incident,'' as those terms are defined in the final rule. These incidents may have many causes. Examples include a large-scale distributed denial of service attack that disrupts customer account access for an extended period of time and a computer hacking incident that disables banking operations for an extended period of time."* In no instance can that notification timeframe exceed 36 hours. (https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf).

A critical question to answer is whether a two-step process, with a 36-hour delay, as is currently the case in the United States, causes a material drawback for regulators in dealing with potentially systemic security issues arising from critical third parties. Regulators receiving simultaneous incident reports from a variety of sources could be an appropriate early warning indicator where time is of the essence. Therefore, simultaneous notification may be the best solution.

However, if a regulator is going to interact directly with third parties, that interaction should take place in concert with both the outsourcer and third party. Absent national security, criminal investigation, or other exceptional circumstances, outsourcers should NOT hear first from the regulator that an incident has occurred at a supplier. Where possible, that initial notification should be provided by the third party to the outsourcer in parallel with any regulatory notification (a community event).

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?

Regulators must agree on a common framework for information sharing and cooperation, as well as agree upon the manner that each will utilize institution-specific (and sector summary) data that each regulator receives – such agreements are gating steps. Notably, whether by design or by default, shared information could include or otherwise reveal highly confidential financial institution or service provider business details, including material, non-public information related to upcoming financial reporting, IPO/investment banking activity, litigation, strategic plans, and even information from active regulatory exams or investigations by the same or other financial authorities. Related, the industry will have substantial concerns that any shared information could trigger additional regulatory review or even reveal compliance failures in other areas of their operations. As a result, clear ground rules that establish proper barriers and restrictions on what is shared or distributable will be necessary to achieve widespread industry acceptance, even as these other risks will always exist to some degree.

Regulators should also agree on a common methodology for designating critical third parties.
The FSB should consider how it might address circumstances in which a group of jurisdictions can reach agreement on critical aspects of cross-border cooperation, but such agreements elude other Financial Authorities. Cross border regulatory cooperation progress will not be linear. The FSB might address whether and when progress steps have been sufficient to publicly expose progress that does not extend to all FSB members.

The FSB's continuing focus on cross-border cooperation, in and of itself, will serve as a catalyst for establishing more effective, cooperative processes. In fact, collaboration and information sharing can serve as levers that allow regulators to encourage the development of robust resilience requirements around systemically critical third parties. Among the issues to be considered are:

- Data security – including data protection techniques that ensure data will not be compromised. This may be a challenge as encryption techniques evolve (e.g., quantum encryption).
- Data governance issues, including but not limited to:
  - Clearly defined limitations of data use.
  - FI-initiated limitations on data sharing and defined circumstances, if any, under which such limitations might be appropriate.
  - Data confidentiality assurance to address competitive concerns, among others – whether authorities can keep data secure.
- Efficiency issues due to differences in systems and programs.

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 and [sic]?

Yes. Cross-border information sharing among financial authorities will be helpful if properly managed. There could be value if the focus is on identifying and mitigating systemic risks and careful consideration is taken on how and what information is shared. This approach requires that regulators be motivated to set the goal to establish and maintain formal agreements across international boundaries where rigor of standards and reporting metrics are harmonized.

Any approach to supervisory authority involvement would be most effective if it is applied sector-wide and takes into account: (1) what can be outsourced (i.e., is already taking place in various jurisdictions globally); and (2) development of widely-accepted reporting formats. That would allow for a 'do it once and spread the results' approach that fosters benefits and reduces compliance costs and fatigue. This approach requires that regulators be motivated to set the goal to establish and maintain formal agreements across international boundaries where rigor of standards and reporting metrics are harmonized.

As a start, we recommend a review of the full range of testing processes that are currently being applied by firms in order to guide robust testing hygiene and reporting processes and reporting (as appropriate). For example, SWIFT has historically managed a mandatory annual cold start resilience test with their largest members every April. SWIFT has routinely shared the results from these tests to all interested members, including smaller members that may be unable or unqualified to participate in such testing, achieving greater transparency for operational resilience standards across the industry entire marketplace and its regulators. Similar, well-designed and broadly based FI-led proposals for testing protocols, schedules, and participants can serve the larger community of firms in scope for critical third-party services. (This example also speaks to the potential merits of pushing the industry in parallel to propose a cross-regulatory reporting framework.)

An example of the high quality that can be gained from examining such processes, third party connectivity mapping is a foundational process that we recommend as a key requirement prior to scenario testing, especially cross-border where unneeded connections—such as those from testing environments that have not been discontinued/disconnected—can unnecessarily complicate resilience testing processes.

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?

Yes. We recommend conducting joint exercises of third (and N^{th}) parties with international reach such as business process outsourcing (BPO) firms, cloud service providers, and payments services providers, among others.

As indicated in FSB Annex 2: Regimes, pursuing supervision of certain critical third-party services and/or service providers, one of the major prongs of DORA is a regulatory review oversight framework that provides a useful model for regulators. We support a DORA-like regime with joint exercises between FI customers and competent authorities with designated leads (e.g., participation by other regulators and a leading FI, such as an EU central bank) that conduct exercises with customers. DORA Article 40 provides specific guidance.

Regulators have the ability to incentivize these activities and therefore improve the future resilience of the sector through this process. It would be valuable for FSB to build on forms of cross-border testing, such as Quantum Dawn and G7 Activities Group, as these are increasingly applied for complex scenario testing and have already been taking place on a voluntary basis. Because financial and insurance firms, supervisors, and third parties are already involved in these exercises, advancing this methodology would facilitate implementation of the Consultative document processes. As continuous monitoring is widely accepted in today's complex and dynamic environment, Financial Authorities should have a specific focus on testing the effectiveness of critical third parties' continuous monitoring programs, as well the effectiveness of continuous monitoring programs sector-wide.

Enforcement and compliance with resulting recommendations should not fall to FIs. Any approach for following such recommendations with respect to each critical service provider should ensure flexibility appropriate to the circumstances; accordingly, this should follow the proposal's overall recommendation of proportionality based on the relationship between the individual FI and the provider.