



afme/

asifma

sifma

August 22, 2023

Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel, Switzerland
Submitted via email: fsb@fsb.org

Re: Third Party Risk Management and Oversight

On behalf of the Global Financial Markets Association (“GFMA”)¹, which consists of the Association for Financial Markets in Europe (“AFME”), the Asian Securities Industry and Financial Markets Association (“ASIFMA”) and the Securities Industry and Financial Markets Association (“SIFMA”) (collectively, the “Associations”), we appreciate the efforts by the Financial Stability Board (“FSB”) and welcome the opportunity to respond to the Consultative Document (“CD”), “Enhancing Third-Party Risk Management and Oversight,” with input and feedback from our collective memberships around the world.

Overview

We are generally supportive of the various tools and practices that the draft toolkit presents for consideration by financial institutions (“FIs”) and financial authorities (“FAs”). The Associations support the promotion of centralized third-party risk management (“TPRM”) functions within FIs, the toolkit’s focused approach to the management of critical services provided by third parties, including those with cross-border impacts, and the proposal’s desire to reduce regulatory fragmentation. We believe these goals support global financial stability by improving the ability of FIs and FAs to monitor and protect against the risks posed by third parties. Without global cooperation, jurisdiction-specific regulation and oversight of global services and risk management programs can lead to inconsistent supervision of issues that can have a systemic impact.

The tools outlined in chapter 3 regarding FIs’ TPRM generally reflect existing FI practices and, when applied in a proportionate, risk-based manner, enable appropriate tailoring of TPRM and oversight activities. We encourage FAs to view the tools in this chapter not as mandatory requirements, but as potential approaches for a FI TPRM program, and to avoid the introduction

¹ The GFMA represents the common interests of the world’s leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. The Global Financial Markets Association (“GFMA”) brings together three of the world’s leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA.



afme/

asifma

sifma

of new concepts or definitions which add unnecessary complexity for FIs and are not focused on financial stability risk.

FI TPRM programs and related regulation and supervision have matured considerably in recent years. FIs have well-established TPRM controls in place to mitigate the risks relating to outsourcing and third-party relationships, including cybersecurity, information technology, data privacy and concentration. Conversely, the area requiring further work and international cooperation is regulatory and supervisory approaches regarding critical third parties to the financial services sector, which are progressing at significantly different rates globally and present real new risks to regulatory and operational fragmentation. The FSB should focus its work on helping develop frameworks for these critical third parties that are not already subject to existing robust rules, regulations, and oversight. Furthermore, as substantial differences in local frameworks would reduce, rather than enhance, the resilience of the financial system, the FSB is well placed to encourage and drive cooperation and convergence in FAs' efforts to address systemic risks posed by certain third parties to the financial services sector.

With respect to the specific parts of the toolkit in the CD, we have identified six key aspects to raise for the FSB's continued consideration:

- **Critical services should focus on risks to FI safety and soundness and financial stability.** We support an enhanced focus on “critical services” provided by third parties and the FSB's efforts to establish interoperable concepts or definitions across jurisdictions. However, it is crucial that differing approaches to materiality assessments do not unnecessarily expand the scope of activities considered as “critical services,” as this would divert valuable resources from addressing third-party arrangements which present real potential risks to the viability of an FI or its critical operations. Therefore, the scope of critical services subject to the toolkit should be limited to those services provided by third parties that, if disrupted, could impair an FI's safety and soundness and create risks to financial stability.
- **The Associations support the principle of proportionality.** In terms of an individual FI's management of its third-party risks, we believe that this principle rightly recognizes that different third-party services require different levels of risk management. Proportionality also means that FAs should consider that the same third party may have a different impact on the operation of different financial institutions and FIs must have the flexibility to approach their relationships with third parties in a manner commensurate with the idiosyncratic risk presented by a specific third-party arrangement.
- **The focus on key nth-parties should be limited to material subcontractors.** FAs should recognize the real limitations in an FI's ability to gather data from third parties on their entire subcontractor population, which could run into the thousands with many providing negligible support. In this regard, the toolkit's suggestion for a standalone risk rating of a critical service provider's supply chain would add unnecessary complexity without real-world risk management benefits. We agree that it is important for FIs to monitor risk generated in their third-party supply chains. Monitoring all nth-parties, however, is an unrealistic and unworkable goal which would detract from a focus on the

most relevant risks in an FI's supply chain. Instead, FIs—and their FA supervisors—should focus on key third parties or “material subcontractors,” which are those subcontractors providing a material part of a contracted service supporting a critical or important function, whose disruption or failure could lead to material impact to service provision.

- **FAs should not seek to engage in oversight of third parties indirectly through the supervision of FIs; oversight of third parties by FAs should occur through direct means where appropriate legal authority is available.** FAs should engage in direct oversight of third parties where they have the legal authority to do so directly, rather than seeking to do so indirectly through supervision by FIs. The CD contemplates that frameworks that provide for direct oversight of critical service providers may produce recommendations from FAs to the third parties on specific services. Any resulting enforcement and compliance obligations from those recommendations should not fall to FIs. In addition, recommendations should be consistent with the principle of proportionality, as FIs should be allowed to retain the flexibility to tailor their interactions with the third party to fit their needs and broader risk management programs.
- **The FSB should ensure that any direct reporting to FAs by third-party service providers is accompanied by safeguards for FIs.** The FSB should consider how direct supervision of third parties by FAs could impact the supervision of FI's. In particular, the interaction of direct incident reporting by third parties to FAs and reporting requirements for FIs should be designed such that it avoids conflicting reporting and confusion in messaging. The third parties should remain obligated to notify relevant FIs of potential material impact on agreed service levels. Any specific information FAs need on FIs that are clients of a critical third party should come through the existing FI regulatory and supervisory framework and not through the third party.
- **The FSB can aim for greater cross-border regulatory cooperation.** The FSB should more clearly define what it views as an achievement in its pursuit of interoperability. The CD's only interoperability goal appears to be avoiding conflicts of law issues. Regulatory interoperability is a desirable outcome, but the FSB should be more ambitious in its efforts to promote international cooperation and cohesion. For example, at a minimum the FSB should push global FAs to adopt common fields and terms for the collection of FIs' third-party data; otherwise, even improved information sharing loses its utility. To that end, we encourage the FSB to take a similar approach as it did with FIRE and advance a post-toolkit workstream specifically designed to align third-party data collection systems.² The objective of cohesion in data collection is to enhance regulatory cooperation; if regulators are working off of a common set of information, it will improve the outcomes of the proposals for cooperation in chapter 4 of the CD, including information sharing and tabletop exercises.

² See FSB, *Format for Incident Reporting Exchange (FIRE)*, (Apr. 13, 2023) <https://www.fsb.org/wp-content/uploads/P130423-2.pdf>.

While there have been legal developments in direct third-party supervision and oversight in some jurisdictions, in many jurisdictions the legal authority supervisors have to oversee third-party service providers directly is less clear. In developing cross-border approaches to TPRM, we encourage the FSB to keep in mind these limitations and perhaps consider an assessment of the kinds of powers that FAs should have with respect to service providers before considering how those powers can be used on a global basis.

The FSB has invited feedback on this CD and, in particular, on the questions set out below. The following comments are the Associations' responses to the questions the FSB posed.

Consultation Questions

Chapter 1 – Common Terms and 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?*

- In general, the definitions presented by the FSB are clear and include the appropriate terms. One term, however, raises particular concern and should be further refined.
- The term “critical service” should be revised to: (i) avoid potential confusion of what this term intends to capture; and (ii) ensure an appropriate scope and criteria to identify third-party services which could significantly impair an FI’s safety and soundness and create risks to financial stability. Other services should be out of scope.

In particular, the toolkit defines a “critical service” as “[a] service whose failure or disruption could significantly impair a financial institution’s viability, critical operations, or its ability to meet key legal and regulatory obligations.” We believe that the phrase “or its ability to meet key legal and regulatory obligations” should be removed, as this would inappropriately broaden the range of services captured by this term/category.

While compliance with legal and regulatory obligations is an important input into the overall risk assessment of a third-party engagement, its inclusion as specific criteria to identify critical services provided by a third party would stray from the intention of the type of risks and related services intended to be captured. Furthermore, its inclusion could be read rather broadly to mean “any” category of legal and regulatory obligation and would be ripe for inconsistent application across FAs, which would lead to further regulatory fragmentation. For example, there are key regulatory obligations related to HR practices which are important but are not relevant for the identification of third-party services that pose potential risks to an FI’s safety and soundness and financial stability. Its inclusion in this definition would be inconsistent with the intention of this classification; instead, **“critical services” should only include those services that will have a material impact on an FI’s safety and soundness and on broader financial stability.**

In addition, the definition of “critical service” also raises concerns and potential ambiguity on what it specifically looks to define. In particular, whether this is intended to

define the criticality of services provided by third parties or the criticality of an FI's own internal services, the latter of which is subject to robust existing definitions and regulatory requirements. To avoid any confusion in this area, we recommend that the FSB update this term to be a **“critical third-party service”**, defined as **“[a] service whose failure or disruption could significantly impair a financial institution’s safety and soundness or critical operations and create risks for financial stability.”**

- We agree with the definition of third-party service relationships and that these do not include services related to:
 - Correspondent banking
 - Lending
 - Deposit-taking
 - Provision of insurance
 - Clearing and settlement
 - Custody services

Those relationships are already subject to more targeted risk management frameworks which capture the nuances of these services.

Chapter 2 – Scope and General Approaches

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

- As discussed in the Overview and elsewhere³, we believe that the general approaches of the toolkit are appropriate, but we encourage the FSB to focus its efforts on systemic third-party risks rather than individual TPRM practices that do not present financial stability risks.
- We support the FSB’s approach to critical services in this section and encourage the remainder of the toolkit, including the definition of “critical service” as described in chapter 1, to align with the scope outlined in the opening lines of section 2.1. That is, to ensure an appropriate scope and criteria to identify third-party services which could significantly impair an FI’s safety and soundness and create risks to financial stability.
- Similarly, we appreciate the FSB’s acknowledgement that criticality (or risk rating) of common third-party services leveraged by FIs will legitimately differ, based on each FI’s usage and business model, among other factors. This point is important not only in terms of supervisory expectations of an FI’s own risk management, but also the outputs of FAs’ direct oversight of certain third parties. For example, future supervisory expectations for FIs linked to recommendations made in connection with new direct oversight regimes for critical third parties, and certain of their services deemed critical to the financial sector,

³ GFMA, *Proposed GFMA principles regarding Critical Third Parties*, (June 2022) <https://www.gfma.org/wp-content/uploads/2022/06/proposed-gfma-principles-regarding-critical-third-parties.pdf>.

should remain subject to the specific relationship between a particular FI and a service provider.⁴ As each FI's usage of a third-party service may differ – including third-party services deemed critical at the system level – any supervisory recommendations with respect to a particular third-party service should serve to better inform an FI's supplier selection, oversight, and overall risk management rather than mandate a one-size-fits all application across every FI.

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

- As discussed in the Overview, we believe that interoperability should be a minimum goal for cross-border cooperation and that the FSB can and should encourage FAs to work together more closely.
- We support the proportionate approach the proposal takes to in-house intragroup services, as they represent a much lower risk than if the same service were done by a third party outside of the group. We are concerned, however, that the FSB's inclusion of intragroup services will overly broaden the scope of the toolkit. Intragroup risks are already the subject of extensive sets of regulation and guidance, and we believe it would be inappropriate to try to add on additional frameworks that are not tailored to the specific considerations of intragroup interactions. For that reason, we would urge the FSB to focus its work on a consistent framework with respect to those third-party service providers that are not otherwise covered by existing standards.
- We appreciate the FSB's support for the use of intragroup services to centralize the use of services ultimately provided by third parties outside the group, which promotes cohesion and resilience within financial groups. We agree with the FSB that regulatory fragmentation limits the benefits that can be provided by a centralized TPRM function. Reducing regulatory fragmentation can thus support TPRM efficiency and outcomes among FIs.

4. *Is the discussion on proportionality clear?*

- We commend the FSB for seeking to incorporate the principle of proportionality throughout the CD as it is an appropriate principle to guide FAs' supervision of TPRM. For example, the proposal rightly clarifies that a service's criticality will justifiably vary from one financial institution to another due to differences in their own business operations and service usage. Although we believe that the discussion of proportionality is generally clear, we also believe that FAs and FIs could benefit from examples of what the FSB believes would and would not be a proportional approach to TPRM. Otherwise, it is possible that FAs in different jurisdictions will take opposing views of what

⁴ See e.g., *Digital Operational Resilience Act*, Regulation (EU) 2022/2554; *Operational resilience: Critical third parties to the UK financial sector*, Bank of England/PRA/FCA Discussion Paper (DP3/22); MAS Financial Sector Cloud Resilience Forum (Apr. 5, 2023).

proportional TPRM should mean. For example, the European Supervisory Authorities have proposed a technical standard that takes the view that a proportional approach to material subcontractors is to include under that umbrella *any* subcontractor linked to a critical or important function, regardless of the actual role the subcontractor plays in the contracted service.⁵ Such inconsistencies can lead to effectively impossible compliance challenges for FIs, and the FSB should seek to provide examples of proportionality in practice so that these challenges can be minimized.

- In addition, we urge the FSB to consider additional areas of the toolkit where its current discussion of proportionality can be reinforced. For example, the FSB could use the principle to remind FAs of the central role of the FI in the management and reporting of risks resulting from a third-party outage or incident.

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 identify critical services? Do these tools rightly balance consistency and flexibility?*

- The proposal is right to focus primarily on critical services provided by third parties, given that non-critical services are far less likely to lead to issues of systemic concern and the aggregation of critical services leads to systemic risk. As a result, we believe it is crucial to be able to identify those third parties that provide critical services. We support the FSB’s proposed adoption of a common framework for the identification of critical services and believe that the direct incorporation of the operational resilience concept of service ‘impact tolerance’ into the TPRM scoping criteria is appropriate.
- We commend the FSB for avoiding a prescriptive approach and instead providing high level considerations. This approach is an appropriate application of the principle of proportionality and enables an FI to identify the services that are most critical based on its operations and risk profile. We believe a similar non-prescriptive approach would be most useful for refining the CD to increase its focus on the identification and management of systemic risks. For that reason, a mandated taxonomy or granular methodology for identifying critical services should be avoided. Instead, as discussed in response to question 7, we believe that consistency is best supported by improving the consistency of data collection.

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?*

⁵ See European Supervisory Authorities, *Consultation paper on RTS to specify the policy on ICT services performed by ICT third-party providers*, (June 19, 2023) <https://www.eiopa.europa.eu/system/files/2023-06/5.%20COP%20-%20Draft%20RTS%20on%20policy%20on%20the%20use%20of%20ICT%20services%20regarding%20CI%20functions.pdf>.

- As discussed above, we believe the draft toolkit provides a useful set of tools and practices for FIs to consider which reflect existing regulatory expectations and FI risk management programs.
 - We encourage the FSB to support the more widespread adoption of pooled audits of service providers. In particular, we support expanding the use of pooled audits beyond just smaller FIs. Pooled audits will improve the efficiency of TPRM for service providers that serve a number of FIs by improving the uniform information for both FIs and FAs.
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?*
- We are supportive of greater consistency in the data that FAs collect on FIs' third-party relationships ("registers"). We believe that doing so can lead to greater regulatory alignment and increase the availability of FIs' resources to be used towards other risk-management priorities. Currently, significant FI resources are dedicated to administrative work stemming from ever-changing – and growing – data requirements on outsourcing and third-party registers. The result is FIs being in an ongoing state of remediation and never in a place of stability, where risk managers can focus on truly value-add activities for TPRM programs.
 - In addition, consistent data collection and information flow can improve the interoperability of the FA supervision of third-party risks, which would likely be a significant benefit to global financial stability. FAs could avoid the delay and confusion that would result from efforts to transcribe data collected in one jurisdiction into a format that can be analyzed in another. As a result, knowledge of issues and growing risks would be able to be transmitted much more quickly.
 - It is our view the underlying supervisory objectives on third party risks, and in particular critical third parties, are similar enough to warrant a more ambitious goal of ensuring interoperability – harmonization of third-party register information and format should be pursued by the FSB on the back of the toolkit's finalization.
 - The proposal, however, does not explain the work required to achieve such an outcome. There are certain common considerations that require consistency, including data fields, data standards, and the approach to proportionality. Consistent data fields will ensure that information that is transmitted between FAs can be of use immediately. Consistent data standards support the flow of information between FIs and FAs and reduce the need to spend time cleaning or reinterpreting data. A consistent approach to proportionality will ensure that FIs and FAs have a uniform view of the kinds of issues and risks that warrant transmission, which will prevent distraction and focus risk management attention where it is most useful. Global alignment on these key considerations is possible and would be beneficial to FIs, FAs, and global financial stability.
 - Furthermore, we urge FAs to work constructively with each other on enabling frameworks for cross-border data flows, such as for example the Singapore-US Joint

Statement on Financial Services Data Connectivity⁶, the Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas (BSP) and The Monetary Authority of Singapore⁷, and the Singapore-UK Digital Economy Agreement⁸.

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 support the FSB’s approach of addressing risks associated with service providers’ supply chains in a risk-based manner. As noted in the CD, “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.”

As discussed above, oversight targeting every subcontractor or nth-party is not only impractical (it is not feasible to break down every third-party provider through a vertical service approach), but would also divert valuable risk management resources from subcontractors that present the most relevant and material risks to the contracted service.

For that reason, we support the FSB’s focus on key nth-parties or “material subcontractors.” To avoid inappropriate interpretations of this concept, however, we encourage the FSB to clarify that a key nth-party or material subcontractor is a service provider of a third party providing a material part of the contracted service supporting a critical service, whose disruption or failure could lead to material impact to service provision.

- For these same reasons, we do not support the FSB’s proposal that FIs could adopt a separate third-party supply chain risk rating. Such an approach would not prove meaningful to actual risk management and would merely serve as a time-consuming compliance exercise. FIs should not be encouraged to manage third-party supply chain risks in isolation and, as discussed above, an FI’s ability to gather sufficient information to create such a rating is highly limited. Instead, third-party supply chain risks should be considered a piece of the FI’s broader TPRM program.
- Generally, as part of the contractual agreement with a third party and where it’s possible and practical, any obligations set for the third party are required to be cascaded to any

⁶ MAS, 2020: <https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity>.

⁷ MAS, 2020: <https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas#:~:text=16%20November%202020-,Joint%20Statement%20of%20Intent%20on%20Data%20Connectivity%20between%20Bangko%20Sentral,The%20Monetary%20Authority%20of%20Singapore&text=1.1.,development%20of%20the%20financial%20sector>.

⁸ Ministry of Trade and Industry Singapore, 2022: <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA>.

subcontractor utilized as part of the contracted service. A specific control is also included in these agreements to require that the third party operate a robust TPRM program of their own to ensure oversight and enforcement of those obligations. As part of due diligence performed during onboarding, and on an ongoing basis throughout the lifecycle of the third-party relationship, an FI will assess the third party's TPRM program to confirm adherence to this control requirement. This provides a more effective means to address risks across the third party's supply chain.

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 urge the FSB to ensure that the concepts of continuity, exit, and resilience planning are not conflated within the toolkit as seems to have been done in certain places. These plans are designed for different stages and events in the lifecycle of a third-party relationship and as a result have different considerations that make them effective. We also believe that the FSB and FAs can draw significant value from work that has already been done with respect to FI resolution and recovery planning obligations. These plans already require FIs to identify those services and service providers that, if disrupted, would pose a serious challenge to the FI's operations and viability. A similar approach can be incorporated into an FI's business continuity planning.

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 that it is important to separate concentration risk from related risks (e.g., substitutability), as FSB has done, because these risks require different approaches for identification and management. Concentration in itself is not inherently bad and can generate certain advantages, including reduced complexity and easier management and control of a smaller number of parties. We recognize, however, that dependencies due to concentration can impact the safety and soundness of an FI and its operations in the event of a major failure. We note that while FIs generally already assess and address their own third-party concentration risk as part of their ongoing operational resilience, they are unable to assess accurately the risk posed to systemic financial stability.
- We also support the FSB's focus on mitigating the risks associated with concentration and concentration-related risks and that it does not introduce a common one-size-fits all approach for "concentration risk." We encourage the FSB to note in this section, as it does in section 4.3, that mitigating actions by FIs and third-party service providers should be taken into account in the determination of concentration risk. The determination, therefore, should focus on the residual risk presented by concentration at the individual FI level.
- Although we acknowledge that both critical and non-critical services should be considered when assessing concentration risk, we note that although non-critical services

may be disruptive to one aspect of an individual FI's operations, they are unlikely to pose a systemic risk if interrupted. Equal weighting or importance therefore should not be given to potential impacts to non-critical services.

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

- We support the FSB's recognition that there is no one-size-fits-all approach to exit planning. Exit plan effectiveness is primarily enhanced by bringing together decision-makers across the FI to agree on what measures to take. Although the proposal questions the usefulness of exit strategies linked to critical services implemented over longer time periods, we believe that such longer-term strategies are an appropriate tool for financial institutions to have in their toolkit given differences in the ease with which third-party relationships can be terminated. In longer-term exit strategies, it is important that financial institutions have additional mitigation plans in place in the event of a disruption.
- Relatedly, it is important for the FSB and FAs to recognize that there are certain situations where exit planning is not appropriate and where FIs need to instead engage in thorough resilience and business continuity planning. For example, cloud services are more suited to resilience planning than exit planning because the difficulty in assessing the "nth-party" dependencies any deeper than the service provider itself makes finding a substitute provider more challenging.

Chapter 4 – Financial Authorities' 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?

- We believe that the scope of the term "systemic third-party dependency" is overly vague, especially given that the determination is up to a single FA. It does not have a clear analogue in the TPRM frameworks that have been adopted in different jurisdictions, including for example DORA⁹ or the Bank Service Company Act¹⁰. This divergence risks adding an additional layer of confusion to the global approach to TPRM.
- That said, we support the FSB's position that a systemic third-party dependency does not automatically equate to systemic risk as we believe such a position could draw unnecessary regulatory and FI attention to dependencies of uneven risk. We appreciate the three-step approach that the FSB proposes for FAs to identify systemic risk, including that mitigating actions by FIs and service providers should be taken into account. The recognition of mitigating actions properly leads to a focus on residual risk, which is a more realistic and appropriate approach. We also believe that this approach is aligned

⁹ *Digital Operational Resilience Act*, Regulation (EU) 2022/2554.

¹⁰ 12 U.S.C. § 1861, *et seq.*

with the principle of proportionality in recognizing that different service provider disruptions will result in different levels of risk.

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

- We discuss our views on proportionality and the identification of systemic third-party dependences above in our response to question 12 and below in our response to question 14.

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

- We urge the FSB, in line with its focus on proportionality, to keep in mind that not all disruptions to third-party services are systemic. As a result, the FSB should avoid including non-critical services in the assessment of third-party services that pose a potential systemic risk. While non-critical services may be disruptive to one aspect of an individual financial institution's operations, they are unlikely to pose a systemic risk if interrupted. Limiting this assessment to critical services, should also allow FAs and FIs to pay closer attention to those third parties that pose the greatest risk.

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 that any reporting on incidents at third parties should come from the FIs, rather than directly from the third parties. FIs are generally already obligated to share incidents that pose a risk to their operations, which means that FAs will already learn of those disruptions that pose a systemic risk. Third parties also cannot share the real and real-time impact that a disruption is having on a FI, because the FI will have adopted mitigation strategies and the third party will at most learn of the impact of the disruption from the FI. As a result, a third party sharing this information is likely to cause confusion and distraction either because the FI will have already shared the information or because the incident did not pose a real issue for the FI. In addition, even if a third party rightfully reports a disruption that is impacting an FI, the third party will at best be providing a duplicative report that may further slow an effective regulatory or supervisory response. This is not to say that we are opposed to third party and FA interaction, but direct incident reporting poses many risks and may undermine the regulation and supervision of FIs.

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?

- As discussed above in our response to question 7, we believe that the inconsistent approach to data among global regulators poses a serious challenge to cross-border

cooperation and information sharing. We urge the FSB to tackle this challenge by proposing specific uniform standards for third-party data registers.

- Separately, we encourage FAs that seek to establish new direct oversight frameworks for critical third parties at the national level to engage in early and strong coordination of these efforts. Just as many FIs provide their services on a cross-border basis, many third parties provide their services to FIs (and outside the financial services sector) on a global basis. It is therefore highly likely that FAs in different jurisdictions designate a third-party entity, or certain of its services provided to the financial sector, as critical. As part of these new oversight frameworks, it is expected that certain recommendations or requirements will be placed on the critical third party; without close coordination amongst FAs, there is a real risk of regulatory fragmentation from differing or conflicting recommendations. For instance, if third parties are bound by specific technology controls or if the regulatory framework is not technology neutral, there could be significant implications for the security and control environments of all FIs using that provider, not only those in that FA's jurisdiction. This would place FIs, and critical third parties, in an untenable position and risks creating additional operational risk and lowering resilience capabilities across both participants.

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?

- We cover this topic in our response to question 18, below.

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?

- We believe that certain forms of information sharing could be particularly helpful for improving cross-border cooperation. For example, if there is an outage of a critical service provider that begins in one region and is likely to move to other regions, it would be helpful if FAs shared that information with each other to develop a global response and promote readiness in other regions of the world. This type of information sharing also suggests that it would be helpful for FAs to engage in advanced planning of how certain service disruptions may be mitigated so that they are prepared when such a situation arises.
- However, we also caution against the oversharing of detailed information on how an outage is affecting a specific FI. FIs are already required to share information about service disruptions with their home regulators and host regulators in jurisdictions affected by the disruption. Sharing this kind of information beyond impacted localities will likely cause FAs in unimpacted regions to make inquiries that are an unnecessary distraction for that FA and the FI.
- The FSB and FAs can also help bring together FIs and third-party service providers in industry resilience exercises to evaluate how real-world scenarios would impact



afme/

asifma

sifma

operations and recovery, which has already proven useful in some jurisdictions and at the global level, for example the GFMA Quantum Dawn¹¹ exercises, the UK-US System Integrity Reconnection Exercise and the U.S. Treasury OCCIP Hamilton tabletop CSP Exercise for large FIs. Such exercises and testing would allow all concerned parties to better understand roles and responsibilities, identify any potential gaps in these relationships, increase collaboration, and ultimately strengthen the resilience of the overall system.

- We also acknowledge that in many jurisdictions the legal authority supervisors will have to supervise service providers is less clear. As a result, the FSB and FAs will need to take into account the degree to which cross-border cooperation in this area will be possible.

We appreciate the opportunity to share our views on the FSB's TPRM toolkit and look forward to continuing to engage with the FSB and global regulators to improve the FI viability and financial stability. If you have any questions on our response or would like to discuss our views further, please contact Melissa MacGregor at mmacgregor@sifma.org or Allison Parent at aparent@gfma.org.

Sincerely,

Allison Parent
Executive Director
GFMA

¹¹ GFMA: <https://www.sifma.org/resources/general/fact-sheet-quantum-dawn-6/>.