Microsoft

Microsoft response: Enhancing Third-Party Risk Management and Oversight

22 August 2023

Microsoft would like to thank the Financial Stability Board for the opportunity to provide comments on the Financial Stability Board's Consultative document: Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities. At the outset, we support the objective to reduce fragmentation in regulatory and supervisory approaches across jurisdictions and facilitating regulatory interoperability and coordination among respective regulatory bodies.

RESPONSE TO QUESTIONS:

We appreciate that the FSB has developed a toolkit for financial authorities and financial services institutions as well as service providers for enhancing third-party risk management and oversight. This response contains Microsoft's preliminary views based on the current consultative document and we would welcome the opportunity to provide further comments during the consultation process. This would enable us to bring the benefit of our industry experience (including engagement with customers and with regulators) and our extensive experience in helping shape regulatory response to technological innovation by sharing our perspectives in other markets. Please find below our specific responses to the questions that are relevant to us.

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?

We believe that the definitions in the consultative document are sufficiently clear and easily understood.

We propose including and amending (as appropriate) the following important terms and definitions:

"Third-party service relationships", "supply chain",[N]th-party service provider , and "systemic third-party dependency".

We propose the inclusion of "critical services" in the original definition of "third-party service relationships", "supply chain" and "systemic third-party dependency".

By covering not only "services" but specifically focusing on "critical services," the definitions would provide a more targeted approach to risk management, operational resilience, regulatory compliance, strategic planning, and vendor management within third-party service relationships. Further, the term "[N]th party service provider is overly broad as it is not narrowed to such providers that provide critical or importance services (or as defined in the FSB paper, a "critical service"), where a dependency on such a firm may materially disrupt or impair the provision of "critical service." Otherwise, it would encompass non-material and non-critical providers that would not have risk of significant impact on the delivery of a critical or important service.

In the subsequent definition of "critical service", the toolkit clearly conveys the potential impact of a critical service's failure or disruption on the financial institution, so this definition would easily fit into the definitions modified as above. However, "failure" and "disruption" should be clarified that it means a "significant and prolonged interruption in delivery of a service, such as failure to meet an SLA.".

"Concentration risk" and "systemic concentration risk": There is no definition for systemic or general concentration risk in Chapter 1 with different interpretations being given to these terms. We would propose the following definitions:

Concentration risk: micro-risk at an institution level where risk of significant failures or disruptions might impact critical business functions of a financial institution.

Systemic concentration risk: events that increase the likelihood of failures or disruptions that would have significant and systemic impact to the financial ecosystem (focused on a macro level).

Chapter 2

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

Yes, the scope and general approaches mentioned in the provided statement are appropriate for addressing third-party service relationships, particularly in the context of critical services and their potential systemic implications.

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

Overall, the scope and general approaches mentioned in the toolkit are appropriate.

4. Is the discussion on proportionality clear?

We agree that the toolkit stresses the need for an effective but proportionate assessment of all third-party service relationships involving the provision of critical services to financial institutions, but further, it should be narrowed to critical services supporting critical or important functions of financial institution business processes – not use for all forms of outsourcing. This approach recognizes that not all service relationships have the same level of impact on financial institutions and aims to avoid undue burden on service providers and financial institutions while ensuring appropriate risk management practices are in place for critical services.

We urge reconsideration of the recommendation in 4.2.2 that service providers grant access to regulators to dashboards or other reporting mechanisms that are used to report service status to customers. Such dashboards contain information specifically tailored for services to customers, not necessarily for government agencies. Further, there are incident reporting requirements for service providers and customers that create situational awareness for regulators.

Chapter 3

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?

Yes, the focus on critical services and critical service providers is appropriate and useful.

We welcome that the toolkit acknowledges the importance of identifying critical services and provides a range of tools for financial institutions to achieve this. Section 3.1 specifically addresses the identification of critical

services and offers guidance on how financial institutions can balance consistency and flexibility in their approach. These tools can be incorporated into existing policies and practices, allowing financial institutions to adapt them to their specific needs while still adhering to a consistent framework.

The toolkit appropriately recognizes that the criticality of services may vary between financial institutions. It encourages regular reassessment of criticality and the consideration of factors such as the service's importance, tolerance for disruption, data security, and substitutability. These tools provide financial institutions with a comprehensive approach to identify and evaluate the criticality of services they rely on.

On page 12, in relation to identifying critical services and their level of criticality, financial institutions should consider the complexity and substitutability, or lack thereof, of a service. The substitutability of a service does not solely depend on its ease of replacement, but also on the level of complexity involved in transitioning to a substitute.

For instance, when substituting one service for another, can the firm manage such service with the right set of skills, resources, procedures, and plans are also available to execute upon this

Section 3.2.1 on due diligence contains a section discussing the '*Level of substitutability of the service and service provider*' on page 14 which can benefit from further clarification. We recommend that this be rephrased to state '*Level of substitutability of the service or service provider*' instead. By using the term "or" instead of "and," it explicitly indicates that the assessment should consider the substitutability of either the service itself or the service provider.

This modification acknowledges that the criticality of a service may depend on both the availability of alternative services and the ability to transition to another service provider. It recognizes that in some cases, the service may be easily substitutable, while in other cases, the relationship with the specific service provider may be more critical or less desirable to replace for a myriad of reasons, including the examples referenced above.

In short, it's not as much about avoiding concentration, rather than on minimizing operational risks (irrespective of concentration).

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?

The provided list of factors for financial institutions to consider during due diligence is comprehensive and covers various aspects of assessing a service provider's capability and risk profile. However, it is important to note that the specific due diligence activities and criteria may vary depending on the nature of the service and the associated risks.

To improve the effectiveness, the toolkit could provide additional guidance on the due diligence process. While the toolkit mentions that financial institutions may conduct appropriate planning and due diligence, providing more specific guidance on the due diligence process would be helpful. This could include outlining the steps involved, the information to be gathered, and the methodologies to be applied. Clear guidance would ensure consistency and facilitate a more structured and efficient due diligence process.

Specific comments on “pooled audits”:

The inclusion of collective assurance mechanisms and feedback from financial authorities in the toolkit is indeed beneficial, especially for smaller and less complex financial institutions that may have resource and

expertise constraints. These measures can help address some of the challenges they face in performing due diligence and monitoring of services and service providers. However, it is worth noting that on page 16 the suggestion is made that collective assurance mechanisms, such as pooled audits may be helpful for smaller, less complex financial institutions. We believe that pooled audits are not the only example due, given these remain highly resource intensive, manual point-in-time exercises that don't allow for continuous assurance and are executed in a manual way and therefore become difficult to scale out to the benefit of larger populations. A globally accepted standard and certification by accredited, independent third parties would offer a more scalable solution. This could involve recommending established frameworks or industry-recognized certifications that are relevant to the financial services sector. Additionally, the toolkit should outline the benefits and considerations associated with using such certifications, including their potential impact on the risk management process and the ongoing monitoring of service providers.

Including guidance on the reliance on third-party assessment services that have no relationship with the third-party provider in the toolkit may also offer more scalable and standardised solutions.

7. What are the potential merits, challenges and practical feasibility of greater harmonization of the data in financial institutions' registers of third-party service relationships?

Greater harmonization of data with a consistent, defined taxonomy in identifying critical and important functions by financial institutions' registers of third-party service relationships can offer several potential merits, as well as present challenges and practical feasibility considerations. Harmonized data would enable easier comparison and analysis across financial institutions, providing regulators and stakeholders with a more consistent and standardized view of the third-party landscape. Harmonized data would also facilitate more accurate and comprehensive risk assessment of critical services, enabling better identification and mitigation of potential risks and vulnerabilities. Finally, harmonization would streamline information sharing between financial institutions and regulatory authorities, allowing for quicker identification of systemic risks and more effective supervisory activities.

However, diverse regulatory requirements and organisational complexities may give rise to challenges as well. Financial institutions operate in different jurisdictions with varying regulatory frameworks. Achieving harmonization would require addressing divergent regulatory requirements and finding common ground to ensure consistency across borders. Financial institutions also have different structures, processes, and risk management frameworks. Harmonization efforts would require coordination and alignment across diverse organisational structures, potentially requiring significant effort and resources.

It is also worth emphasizing the importance of granularity in registers of third-party service relationships for effective identification of concentration risk. The registers of third-party service relationships offer great potential for financial institutions and authorities in their efforts to identify (systemic) concentration risk, but only if these registers provide sufficient granularity. If the list is limited to the third-party providers at the organization level this may not be sufficient, especially in case of hyperscale cloud providers, to assess where concentration occurs.

As regards the practical feasibility, achieving greater harmonization would necessitate collaboration and coordination among financial institutions, regulatory authorities, and industry stakeholders. Establishing forums, working groups, or industry associations could facilitate the exchange of knowledge and the development of common standards. Regulatory authorities can play a pivotal role in promoting harmonization efforts by providing guidance, promoting best practices, and creating incentives for financial institutions to adopt harmonized approaches.

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 tools mentioned in the toolkit, such as information sharing, contractual provisions, and risk rating in registers, provide a starting point for managing supply chain risks. However, their appropriateness and proportionality may vary depending on the specific circumstances of financial institutions and their service providers. It is essential for financial institutions to assess these tools' effectiveness and adapt them to their unique risk profiles and operating environments.

Applying the toolkit in a proportionate and risk-based manner is crucial, especially when it comes to managing the risks associated with nth-party service providers in the supply chain. The number of nth-party service providers can grow exponentially, making it impractical for financial institutions to evaluate and manage each one individually. Therefore, we very much welcome the call for applying the toolkit in a proportionate and risk-based on page 21.

However, under Section 3.4 and 3.5.1-3.5.4, there is no meaningful scoping, limitation or definition of "key nth-party service providers." As referenced in our comments above, this should be narrowly focused on those nth-party service providers where there is a dependency on delivery or performance of the service that itself is a critical or important function. Thus, we recommend that this should be tied to an appropriate and scoped definition of a "nth-party service provider" where "a dependency on such a firm may materially disrupt or impair the provision of a "critical service." We generally agree with the statement in Section 3.5.1 that "focusing on those nth-party service providers that are knowingly essential to the delivery of critical services to financial institutions or which have access to confidential or sensitive data belonging to the financial institution can be more consistent with a proportionate, risk-based approach" but equally this should be a defining limitation to narrowing the scope of identification of such nth-party suppliers as otherwise this is not manageable for third party service providers or financial institutions to manage.

Under Section 3.7, the statement on assistance requires further clarification: "third-party service providers may provide all reasonable assistance to financial institutions during the transition period following an exit." For standardized services, such as cloud computing, financial institutions have tools to leverage to enable exit of a service. To the extent, however, a financial institution wishes for "all reasonable assistance" beyond such tooling, such as actual for-hire services, it should be clear that these arrangements may require a separate service contract for such assistance and is itself not a standard offering included with the cloud services that are licensed on a subscription basis.

Under Section 3.8, the statement concerning objecting to subcontractors is not feasible: "Contractual rights to assess and consent or object to the sub-contracting of parts of a critical service that may increase risk (see Section 3.5)." This provision is too broad as (i) it fails to narrow a focus on subcontractors performing critical or important functions (as referenced further above in our comments) and (ii) is impractical in allowing any customer to cast a veto right to any subcontractor. Rather, in circumstances where, if identified, a subcontractor providing a critical or important function presents substantial risk that cannot be mitigated against and such risk could impair or disrupt critical functions of a service, a financial institution may terminate such service if the issue is not remediated. Actual rights to "object" would not be practical as it leaves any one financial institution a veto right for any subcontractor (or material subcontractor, which should be the focus).

As noted above, such identification and assessments should be appropriated narrowly and focused solely on material subcontractors providing critical or important functions where dependency is such that a failure by such a subcontractor presents a material risk in the delivery and operational resiliency of the underlying critical service provided to the financial institution.

By adopting a proportionate and risk-based approach, financial institutions can focus their resources and efforts on assessing and managing the key nth-party service providers that are most critical to the delivery of their critical services or that have access to sensitive data. This approach allows financial institutions to prioritize their risk management activities and allocate resources effectively.

Financial institutions can use risk assessment methodologies to determine the level of risk posed by different nth-party service providers based on factors such as their criticality, the nature of services provided, and the potential impact of disruptions. This allows them to concentrate their monitoring and mitigation efforts on the most significant risks.

Furthermore, financial institutions can establish criteria and thresholds for identifying which nth-party service providers require closer scrutiny or additional risk management measures. This enables a more targeted and efficient approach to managing supply chain risks.

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?

Effective business continuity plans for critical services typically incorporate several key elements and best practices, most of which are covered in the consultation.

It is however important to emphasise that cloud service providers (CSPs) face specific challenges when conducting joint business continuity testing with financial institutions as described in bullet 3 of Section 3.6.3 of the toolkit due to the shared operating model. The unique context of shared, virtual multi-customer environments and the need to maintain service contractual levels can make traditional end-to-end testing disruptive and impractical.

Traditional end-to-end testing - where a data center is failed over at regular intervals - is not possible without disrupting certain customers who operate their environment in a single region. Such testing would be disruptive to these customers and would violate agreed service level agreements and that is one of the reasons CSPs will test business continuity at a service level once in production only for environments where they also are the responsible party.

Clarifying the shared responsibility for business continuity plans between the CSP and the customer is therefore also crucial. For SaaS solutions and other cases where the CSP is responsible for business continuity planning and testing, financial institutions can request the test results and documentation to assess the readiness of the CSP's plans. This allows financial institutions to gain confidence in the resilience and continuity measures in place without necessitating joint testing that may disrupt other customers' environments. In other cases, such as IaaS, customers design their critical services in ways that meet business continuity requirements, and they can also assess business continuity for these services end-to-end without involvement of the CSP.

By clearly delineating the responsibilities and expectations regarding business continuity plans, financial institutions and CSPs each can ensure the continuity of critical services without compromising the operational integrity of the multi-tenant environment or violating service level agreements. From a practical perspective, a joint test may also not be necessary and would moreover indicate unclear responsibility over who is responsible for business continuity plans.

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?

Concentration risk is an aggregate term pointing to the higher impact an adverse event would have on one or more critical services. When assessing such risks, one must evaluate each of the underlying threat scenarios, which in turn leads to a nuanced view that includes both benefits and drawbacks associated with concentration of services. Threat factors to consider include data center disasters, hardware failures, network outages, cyber-attacks, faulty changes and upgrades, human errors etc. For each of these appropriate mitigating measures should be carefully considered. Firms must also consider mitigation costs, complexity, and availability of in-house skills when considering the preferential solution for addressing concentration risk.

It may be possible and, in some cases, even desirable to maintain concentration so firms can maximally strengthen resilience. Rather than try and remove the third-party dependency entirely, firms should focus on strengthening operational resilience by addressing the underlying threat scenarios associated with concentration risk (for example: a regional data center disaster event). These scenarios can often be addressed with less drawbacks by *(i)* reducing the probability that the threat event occurs and *(ii)* limiting its impact by reducing concentration:

1. Reducing probability is achieved by strengthening resilience in the solution design. A robust set of risk management procedures can enhance operational resilience despite concentration of critical functions with a single third-party provider. Measures may include running state-of-the-art infrastructure, running a zero-trust security model, and automation procedures which may include patching systems with the latest updates. Each of these contributes towards obtaining a maximally resilient environment.

2. Limiting impact by reducing concentration at lower levels is achieved by designing services to operate across multiple availability zones in an active/active configuration; by ensuring sufficient redundancies and recovery mechanisms are in place (for instance backups), and by leveraging geo-redundant designs. Such configurations not only result in higher resilience and better SLAs, but also help to mitigate against threats such as the loss of a single data center or even an entire region due to their distributed nature. The impact of threats can be reduced, hereby also reducing concentration risk, in some cases even going beyond what is feasible in on-premises or hybrid scenarios. In conclusion, if a full cloud topology offers higher resilience compared to alternatives, concentration risk will also be effectively reduced although concentration itself is not diminished.

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

It would be risky to choose a less resilient technology solution that runs on a hybrid or multi-cloud environment to address concentration risk if the alternative solution is much more complex, difficult to understand, and may otherwise present other risks.

It is not a zero-sum choice of running multi-cloud environments or running certain operations in a single environment with only multi-cloud mitigating overall operational resilience. A multi-sourced environment presents a different set of risks and considerations, including complexity to the environment that may be more difficult to manage. These remain risk-based decisions left to institutions to solve based on capabilities, skills, resources, and other factors.

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, the concept of "systemic third-party dependencies" is clear. It refers to dependencies that are external to a system or organisation, typically involving third-party entities or components. These dependencies can include external software libraries, APIs, services, or any other external resources that are relied upon by the system or organisation for its functioning. The term "systemic" indicates that these dependencies are ingrained or inherent to the system's operations. By using the term "systemic third-party dependencies," it is evident that the text is referring to external dependencies that play a significant role in the functioning of the relevant system.

We would recommend adding "critical services" to the definition as well as further defining what is meant by "disruption" "failure" and "implications for financial stability."

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

Achieving proportionality in the identification of systemic third-party dependencies by financial authorities involves considering the level of risk and impact associated with each dependency.

The relevant steps that can be taken to achieve proportionality can be the following:

- **Risk assessment**: Financial authorities can conduct a comprehensive risk assessment to identify and prioritize systemic third-party dependencies. This assessment should consider factors such as the criticality of the dependency, the potential impact of its failure or disruption, and the likelihood of such events occurring.
- **Categorization**: Dependencies can be categorized based on their level of criticality or importance to the financial system. High-risk dependencies that have a significant impact on financial stability should be given greater attention and scrutiny. A consistent and well-defined taxonomy of what constitutes critical or important functions is important for purposes of identifying in a coherent way which dependencies exist based on critical or important functions of services provided by third party providers that may be deemed "systemic."
- **Differentiation**: Financial authorities can differentiate between different types of dependencies based on their characteristics. For example, they can distinguish between dependencies that are essential for core banking functions versus those that are less critical for day-to-day operations. For example, is email truly critical to core banking functions. In the assessment process of systemic concentration, we recommend that financial authorities should go beyond the identification of third-party providers at a firm level and evaluate the specific services being offered to get a more nuanced understanding of where exactly the systemic concentration occurs. This is partially addressed in Section 4.3.2 at the top of page 34 - bullet 1 - and in Section 4.3.3 but could be expanded upon. There is an increasing dependency on a limited set of third-party cloud providers that has been observed, but these providers often offer many services through a distributed architecture at hyper scale on a global basis. To identify points of concentration we recommend financial services authorities should identify also which services are being used across the system and their criticality to the operating function of the financial services ecosystem. This will require further work on a common taxonomy or nomenclature that is consistent and underlying current reporting requirements on use of third-party outsourcing.
- **Proportional oversight**: The level of oversight and regulation can be proportionate to the risk posed by the systemic third-party dependencies. Higher-risk dependencies may require stricter monitoring, regular audits, and contingency plans, while lower-risk dependencies may be subject to less stringent oversight.

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

The identification and designation of service providers as critical from a financial stability perspective is an important consideration for financial authorities. By designating certain service providers as critical, authorities aim to ensure the smooth functioning and stability of the financial system. We agree with the approach of the toolkit.

To be able to designate, what is "critical" should be objective based on measurable and quantitative criteria. This includes the type of critical services provided (based on a well-defined taxonomy), the scope and scale in in use, including by global or domestically significant institutions, and the level of substitutability of such critical services that are designated.

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?

Generally obligations on reporting to supervisory authorities should remain the responsibility of financial institutions, which is the primary obligation which exists in regulatory frameworks today. Imposing requirements on technology providers to report to supervisory authorities would be a new and potentially complicated regime that risks regulatory fragmentation and complexity and challenging for technology providers to manage across multiple jurisdictions. Thus, we view it as preferable to maintain incident reporting requirements as constituted under applicable law without imposing a new reporting requirement that itself would be unprecedented.

In addition, it is important to define thresholds for incident reporting that are appropriate and aligned to the delivery of critical services. Appropriate means thresholds and boundaries are defined so that only incidents must be reported that have a sufficient level of severity and affect the critical service. The principles of Coordinated Vulnerability Disclosure (CVD) should also be followed in this case, rather than to re-imaging a process tailored to financial services within a specific jurisdiction to avoid a patchwork of reporting regimes being applied to global service providers.

Such reporting principles, at a minimum, should be standardized across jurisdictions to avoid regulatory fragmentation and disparate reporting requirements. Further, these should not be voluntary but based on applicable regulatory requirements mandated by law. And finally, to the extent technology providers are not themselves subject to such reporting requirements directly, a mechanism of mandating such requirements to financial institutions, which remains the primary mechanism today, is a reasonable approach to obtain such information.

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?

The challenges and barriers to effective cross-border cooperation and information sharing among financial authorities can have significant implications for financial institutions and service providers. We agree with the key challenges that the toolkit identifies, such as differences in mandates, legislation, and organisational structures, practical coordination challenges and sharing sensitive information.

We place emphasis on regulatory cooperation. To the extent that a service provider is designated a "critical" and subject to supervision in more than one jurisdiction, authorities, and the service provider a like may benefit from regulatory cooperation and oversight in the context of sharing of, and oversight, of such third

party. Such services, when standardized, do not warrant separate examinations and are both costly, duplicative, and not scalable. As in the case of "pooled audits," pooled regulatory examinations should be a consideration amongst regulators who themselves have limited resources for such examinations.

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?

We welcome that the toolkit acknowledges the value of cross-border information sharing among financial authorities and recognizes that effective cross-border supervisory cooperation and information sharing can support the regulation and supervision of internationally active financial institutions' third-party arrangements. As regards the challenges pertaining to such information sharing, please see our answer re question 16 above.

Regarding cross-border resilience testing and exercises, we appreciate that the toolkit highlights the importance of involving internationally active service providers in such activities. Bringing these service providers into future cross-border and sector-wide exercises, and potentially cyber resilience tests, can help strengthen the resilience of the global financial system. As regards the challenges pertaining to pooled audits, please see our answer re question 6 above.

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 welcome that the toolkit suggests several specific forms of cross-border cooperation that financial authorities should consider addressing the challenges. These forms of cooperation aim to enhance coordination, collaboration, and information sharing among supervisors in multiple jurisdictions. We agree with the forms of cooperation proposed by the toolkit. Most importantly, for the sake of greater convergence of regulatory and supervisory frameworks, financial authorities can explore ways to improve alignment of their regulatory and supervisory frameworks on third-party risk management on a cross-border and cross-sectoral basis. Establishing consistent criteria and methodologies for assessing, classifying, and identifying systemic third-party dependencies and potential systemic risks can facilitate the exchange of information and promote more efficient oversight.