INTESA SANPAOLO

Third-Party Risk Management and Oversight
FSB Consultation

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?*

Chapter 2 – Scope and general approaches

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

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

Chapter 3 – Financial institutions' third-party risk management

4. *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?*

A common control framework for third parties monitoring would desirable, declined by scope and technology with recognized and more easily applicable standards contextualized on clients/services.

The creation of regional central control bodies executing controls on the critical service providers and guiding FIs in specific control activities on the third parties (similarly to DORA provisions on oversight of critical third parties by financial sector Authorities).

Financial institutions may also consider the following areas for the identification of critical services and their level of criticality in a banking legal context:

- **the innovative nature of the service;**
- **the ESG (Environmental, Social, and Governance) impact of the service.**

Do these tools rightly balance consistency and flexibility?

5. *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?*

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

In order to prevent registers of third parties to create fragmented regulatory requirements (i.e. for incident reporting) and to become a burden for FI we encourage Authorities to consider common templates and criteria. We suggest the inventory of third parties that FIs maintain to enlist all third parties, the respective the services and functions performed by them, the level of access each third party has to the entity's systems and the type, sensitivity, and location of data maintained or processed by each third party. A starting point for the FSB may be the DORA Register for information.

In a banking legal context, FIs may also use the following aspects in their onboarding and monitoring of service providers:

- **not only the management of cybersecurity/information security, business continuity, and crisis, but also the existence of management systems for these aspects. The management systems should be certified or compliant with internationally recognized best practices;**

- **the presence of an ESG impact management system;**
- **the presence of a recognized CERT/CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team) integrated into a community of CERT/CSIRT.**

7. *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 would suggest adding among the challenges the possible difficulties for FIs (especially smaller ones) to have third parties accept all contractual clauses and provisions in consideration of uneven contractual powers and leverages.

8. *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?
FIs' registers of third-party service relationships should include the [N]th-party service provider within the supply chain that process confidential or sensitive data (including but not limited to personal data) of the financial institution.

9. *How can financial institutions effectively identify and manage concentration and related risks at the individual institution level?*
The concentration risk should be assessed as an indirect criticality towards the third-party service provider, considering also the percentage of the third-party service provider's revenue derived from the financial entity.

10. *Are there any additional tools or effective practices that the toolkit could consider?*

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

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?

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

14. *Are there any thoughts on financial authorities' identification/designation of service providers as critical from a financial stability perspective?*
The factors that determine criticality should include the degree to which the third party supports and has access to critical functions and core business lines.

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?*
Enhanced utility could be derived from significant incident reporting by third-party service providers within the financial sector if competent authorities could establish an efficient and prompt mechanism for sharing information with financial institutions. Alternatively, such reporting should also be extended to financial institutions that are customers of these crucial providers, in alignment with contractual clauses.

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?*

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 support the proposed pooled audits, considering that this can create a win-win situation both for providers and FIs, and can also be leveraged by authorities in case of critical providers.
Furthermore, concerning systemic and concentration risk strategies, it is advisable for pertinent authorities to contemplate the adoption of suitable actions aimed at mitigating these risks and enhancing the exchange of information. These measures could involve consolidating third-party information from various entities and pinpointing potential vulnerabilities like single points of failure, concentrations of third-party involvement, or vulnerable transmission channels.

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?*
Authorities can seek opportunities to work with their respective counterparts in other sectors and forums to promote sound cyber risk management, improve cyber resilience, support the sharing of effective practices and, if appropriate, pursue coordinated responses.