FSB FINANCIAL STABILITY BOARD

4 December 2023

Enhancing Third-Party Management and Oversight

Overview of responses to the consultation

1. Introduction

On 22 June 2023 the FSB consulted on a toolkit for financial authorities and financial institutions for enhancing third-party risk management and oversight. The toolkit focuses on providing a set of tools to enhance the oversight of financial institutions' reliance on critical service providers and includes common terms and definitions on third-party risk management. The purpose of the toolkit is to (i) reduce fragmentation in regulatory and supervisory approaches to financial institutions' outsourcing and third-party risk management across jurisdictions and sectors; (ii) strengthen financial institutions' ability to manage outsourcing and third-party risks and, by extension, the resilience of the financial system as a whole; and (iii) facilitate coordination among relevant stakeholders (i.e. authorities, financial institutions and third-party service providers).

The FSB received 26 responses to the consultation which ended on 22 August 2023. Respondents included trade associations that represent financial institutions (12), regulated financial institutions (5), third-party providers (4) and other (5).

Overall, respondents supported the toolkit's focus on critical services and critical service providers. The flexible, technology neutral and risk-based approach was welcomed, noting that it recognises differences across jurisdictions, and amongst financial institutions and authorities, markets, business models, and legal/regulatory frameworks. Respondents welcomed the comparable and interoperable approach across jurisdictions with the objective to reduce fragmentation in regulatory and supervisory approaches, highlighting its importance for facilitating coordination among authorities, financial institutions, and service providers.

Key areas of feedback were (i) definitions and terms, (ii) supply chain risks and (iii) supervisory cooperation and information sharing.

With respect to definitions and terms, most respondents largely approved the suggested definitions, but some requested further clarifications whilst others called for additional guidance. Some proposals overly reduced or broadened the scope of intended definitions. For a number of concepts, a narrower or more guided definition would reduce the flexibility that regulators would have in defining a suitable approach in their own jurisdictions.

Supply chain risk management was one of the areas of the consultative document that generated the most feedback. A recurrent theme was a request to limit the tools scope to those 'nth-Party Service Providers' that are truly essential for a service provider's ultimate delivery of critical services to financial institutions (referred to interchangeably as 'essential' or 'key' nth-Party Service Providers). Whilst the draft toolkit already endorses a focus on those nth-party service

providers (see section 3.5.1) that are knowingly essential to the delivery of critical services to financial institutions, a number of respondents noted that there is no agreed, consistent definition, limitation or scoping on this subset of nth party service providers.

On supervisory cooperation respondents noted the importance of strengthened cooperation between financial supervisory authorities, including cross-border information sharing as well as testing. The comments detailed the challenges of sharing confidential/sensitive information. Respondents called for enhanced coordination between different authorities, with many responses pointing to duplication or conflicting requirements between differing authorities as potentially, or in actuality, undermining efficiency and resiliency of financial institution's operations.

Having considered the feedback and suggestions received, some amendments and clarifications were made to the final report, including the following changes:

- **Financial institutions third-party risk management:** A clarification on the sharing of responsibilities between financial institutions and third-party service providers has been added which emphasises that regardless of the type of third-party service relationship, the final accountability towards the financial authorities and financial entity's customers remains with the financial entity and its board and senior management. The toolkit for financial institutions was further strengthened through a number of clarifications and changes.

- **Definitions and terms:** A footnote was added to better specify intragroup service providers. Critical services were clarified to mean services to financial institutions.

- **Supply chain risks:** Further clarifications have been added in relation to complexities of supply chains. This included that financial institutions as part of their due diligence should consider the length and complexity of supply chains as an inherent risk, and the need to include robust supply chain risk management in contractual provisions. The risk rating for supply chains as a tool was deleted.

- **Business continuity plans:** The toolkit has been updated to clarify the differences and overlaps between business continuity plans (BCPs), resilience planning and exit strategies.

- **Incident reporting:** Further clarifications on incident reporting have been added. Respondents' feedback was largely relevant to identifying challenges related to direct reporting to financial authorities. Many respondents did not support implementation of direct reporting by third-party providers to financial authorities.

2. Summary of feedback received

2.1. Common Terms and definitions (Q1)

Most respondents largely approved the suggested definitions and terms.

On ‘Third-party service relationships’, some suggested to remove ‘service’, as the concept should focus on the relationship or to remove ‘relationship’ as the concept should focus on the service. One suggested to include Financial Market Infrastructure in the proposed scope of third-party service relationships of financial institutions. One respondent stated that this should only include critical services.

On ‘Service provider’, two respondents suggested to include only material providers in the definition of ‘nth-party service provider’. Several respondents recommended excluding branches from the definition of ‘intra-group service provider’. As they are not separate legal entities services between business units of the same legal entity, they would not be considered intra-group arrangements under established company law in most jurisdictions.

On ‘Outsourcing’, one respondent argued that the definition should not be limited to the services that the financial institution could reasonably undertake itself although this wording features in most authorities’ existing definitions of outsourcing.

On ‘Supply chain’, another argued that the type of service should be included in the definition to avoid the consideration of any type of service.

On ‘Critical service’, several respondents suggested refining the definition to ensure that this concept applies only to service providers to financial institutions and is not mixed up with the financial services that the financial institution itself provides to its customers (e.g. deposit-taking, insurance etc), and that this should be retitled as a “third-party critical service”. Other respondents suggested that this definition only consider disruption from operational risks on viability and critical operations and not include compliance with legal and regulatory obligations, which they viewed as too broad. Another suggested to include ‘critical services’ in the definition of ‘third-party service relationships’, ‘supply chain’ and ‘systemic third-party dependency’ which would be a more targeted approach. Some respondents suggested expanding the list of definitions to include definitions for disruption, substitutability, relevance to financial stability, materiality or (systemic) concentration risk.

On ‘Critical service provider’, two respondents suggested that the definition should be focused only on providers that contribute to a material extent to the critical service, and another commentor requested that it should not include service providers that are readily substitutable.

On ‘Systemic third-party dependency’, some suggested that the definition be focused on the dependency on critical services.

2.2. Scope and general approaches (Q2 – Q4)

Overall, respondents welcomed the general toolkit approach.

Respondents supported the discussion of interoperability, as distinguished from a one-size-fits-all approach. Some comments acknowledged that regulatory homogeneity was an impractical objective, and others noted the benefits of permitting flexibility of approaches to arrive at comparable, outcomes-based results. A few respondents observed that progress on interoperability is likely to be incremental and welcomed further international work to resolve emerging, conflicting regulatory standards. There was wide support for avoiding unnecessary

fragmentation in approaches across jurisdictions, as that would be costly for industry and detracted from a focus on risk management.

Several respondents cited incident reporting as an area of current interest to avoid friction between regulatory regimes. A respondent advocated that the FSB explicitly recommend regulators not establish overly broad or specific incident reporting triggers that might lead to conflict with other regulatory regimes. Other respondents mentioned nth party service providers and outsourcing registers as areas where further work on interoperability would be welcome.

Respondents generally approved of the proportionality discussion. As consultation responses observed, complexity can vary by the type of enterprise. Some asked that certain examples be carefully qualified, and others asked to clarify that the principle of proportionality applies more generally to the toolkit. Some respondents found the example used for proportionality (backup providers) could be misinterpreted. In addition, a few respondents asked that certain regulatory burdens be commensurate or scaled with the level of criticality of a service.

2.3. Financial institutions third-party risk management (Q5 – Q11)

Comments received on critical services and critical service providers (Q5), on tools for financial institutions (Q6), and merits, challenges and feasibility of greater harmonisation of data (Q7)

Overall, the comments from respondents are supportive of the toolkit being focused on critical services and critical service providers as this can help increase common, global understanding of how financial institutions and financial authorities can identify critical service providers. Respondents agree that the toolkit strikes an appropriate balance between consistency and flexibility given the framing as considerations, not requirements. Respondents acknowledged that the draft toolkit provides a useful set of tools and practices for financial institutions to consider which reflect existing regulatory expectations and financial institution risk management programs. On interoperability and reducing fragmentation, one respondent suggested the use of established and audited controls and certifications as a means of reducing fragmentation of approaches.

Comments received on tools for supply chain risks (Q8)

Supply chain risk management was one of the areas of the consultative document that generated the most feedback. This feedback was not strictly limited to responses to Question 8, but also featured in responses to other questions, such as Question 11.

A recurrent theme was a request to limit the tools in Section 3.5 of the toolkit to those 'nth-Party Service Providers' that are truly essential for a service provider's ultimate delivery of critical services to financial institutions (referred to interchangeably as 'essential' or 'key' nth-Party Service Providers. Though some respondents went further and asked for the toolkit to be limited to material subcontractors only. Respondents commented extensively on the practical difficulties that financial institutions face when assessing the resilience of their service providers' supply chain, and the impossibility of individually monitoring every nth Party Service Provider.

Respondents raised many of the challenges faced by financial institutions when it comes to supply chain risk management, which is acknowledged in Section 5.3.1. Whilst respondents noted that financial institutions should assess their third-party service providers' supply chain risk management programme, they highlighted the challenges they face in directly overseeing nth Party Service Providers given they do not directly contract with them. There were a few proposals for potential additional tools to manage these risks, including:

- where possible and practical, contracts between financial institutions and third-party service providers should cascade the third-party service provider's contractual obligations to its nth Party Service Providers; and
- require third parties to operate a robust supply chain risk management program.

Conversely, some respondents noted that giving every individual financial institution a contractual right to consent, or object to the sub-contracting of parts of a critical service would be impossible in cases where standardised services are provided to multiple customers. At most, a financial institution could terminate the contract if it felt that the proposed sub-contracting of part of a critical service by the third-party service provider to an nth Party Service Provider would expose it to an undue, unmitigable level of risk. One respondent noted that continuous monitoring tools offered by a third-party service provider as part of a critical service could help it mitigate supply chain risks.

Some respondents advocated a stronger role for authorities in helping financial institutions managing supply chain risks. Some suggested that authorities should share information on key nth Party Service Providers with firms taken from various data sources (e.g. operational continuity in resolution (OCIR) documentation, incident reports). Others noted that legal or regulatory intervention might be needed to compel third-party service providers to give financial institutions appropriate visibility of their supply chain and manage relevant risks.

There was strong opposition to the idea of a risk register for supply chain, at least as a standalone tool. All but one respondent who commented on this tool rejected the idea.

Comments received on effective business continuity plans (Q9)

Respondents were broadly supportive of the proposed approach in this part of the toolkit. A key recurring theme was the importance of clearly differentiating between business continuity planning, resilience planning and exit strategies. In this regard, respondents noted that:

- there might be limited recourse to feasible exit plans for some critical services. This should be flagged as a risk in itself;
- even where a feasible exit plan has been identified, it may not be workable as a short-term response to the disruption or failure of a critical service or critical service provider;
- the relative time-criticality of different critical services should feature in financial institutions' BCPs. Conversely, one respondent noted (in its response to Q11) that the toolkit should recognise the value of exit strategies that are designed to be implemented over a long timeframe.

Another key theme was on the idea of joint BCP testing between financial institutions and critical service providers in Section 3.6.3:

- Cloud service provider respondents noted that, in light of the 'shared responsibility' model in arrangements for the use of public cloud services, joint testing with individual financial institution customers may not be workable and could blur the respective responsibilities of different parties. Consequently, the idea of joint testing in Section 3.6.3 should be caveated to situations where it is "appropriate to the service being provided";

- Other respondents noted that an effective BCP for critical services should be mutually developed and agreed by financial institutions and their third-party service providers, which would require a completely different approach and higher communication and cooperation between them. Another respondent pointed out that annual disaster recovery testing for suppliers of critical technology services aligns with current best practices.

Some respondents urged authorities to consider how to support financial institutions in mitigating BCP risks, particularly in circumstances involving financial sector critical service providers. In particular:

- One respondent suggested further guidance on industry-wide testing, pooled test results, and reverse stress testing;

- another respondent suggested cross-border recognition by authorities of BCPs done by financial sector critical service providers.

Comments received on concentration risk (Q10)

Comments on this section were broadly supportive of the toolkit's proposed approach. A number of respondents emphasised the importance of financial institutions assessing concentration risks holistically taking into account:

- direct dependencies on third-party service providers;

- indirect dependencies in service providers' supply chain, and interconnectedness (also relevant to the identification of systemic third-party dependencies in Chapter 4);

- the combined effect of disruption to the critical and non-critical services that a single service provider provides. However, one respondent noted that critical services should still be weighted more in this assessment;

- One respondent noted that, in the context of individual financial institutions, concentration could be defined as the risk to a financial institution's ongoing operations (particularly in case of a disruption) due to lack of diversification in providers for a given service (which is what the toolkit focuses on);

- issues relating to vendor lock-in.

Several respondents emphasised that concentration can sometimes bring positive effects (efficiency, improved resilience etc.), which the toolkit already acknowledges. One respondent

emphasised the need for third-party risk management to be considered holistically. Financial institutions should take a balanced view of the potential benefits and risks of using a highly concentrated third-party service provider. Another respondent questioned how financial institutions should manage concentration on intra-group service providers.

In terms of tools for financial institutions to identify and assess concentration risk, one respondent emphasised the importance of the register in Section 3.4. Other potential tools mentioned by respondents included process maps, supply chain diagrams, and other dynamic tools to highlight the risks and resilience of a firm's third-party ecosystem. One respondent suggested that authorities should develop a methodology for financial institutions to assess concentration.

In terms of potential tools for managing concentration risk, there were different views on the merits of multi-vendor strategies. These largely focused on cloud and reflected the divergent views of individual cloud service providers. One respondent suggested provider-specific BCPs and exit strategies as a potential tool for mitigating concentration risk.

Comments received on issues requiring further consideration (Q11)

Overall, most of the respondents did not raise any new or additional points. For the most part, they either restated points raised in the responses to other questions, such as the difficulties for financial institutions in managing nth party and supply chain risks. Some respondent raised the difficulties for financial institutions recruiting and retaining staff to effectively oversee third-party service providers offering complex services, and the need to rely on independent experts to assess these service providers if in-house expertise is unavailable.

2.1. Financial authorities' oversight of third-party risks (Q12 – Q18)

Comments received on identification of systemic third-party dependencies (Q12)

Responses regarding the concept of 'systemic third-party dependencies' varied amongst stakeholders. Many of the respondents were of the view that the concept is readily understood and the scope is appropriate. Some respondents acknowledged that the concept of 'systemic third-party dependencies' is new and may require further work to be better understood.

Conversely, some respondents voiced concerns regarding the concept being overly vague, particularly for financial institutions to determine whether third-party relationships give rise to financial stability risks. Some respondents noted a preference to narrow the scope of the concept through reference to 'critical services' and further definition of terms such as 'disruption', 'failure' and 'implication for financial stability'. Lack of comparability to existing terminology across jurisdictions was also raised as a concern by a respondent.

A few of the respondents highlighted difficulties for financial institutions to identify systemic third-party dependencies. It should be noted that Section 4 sets out that the determination of systemic third-party dependencies would be performed by the financial authority and **not** the financial institution. Section 4.3.1 sets out that what renders a third-party dependency systemic is a financial authority's assessment of the potential impact on financial stability from disruption to the relevant service(s) or service provider.

Comments received on proportionality (Q13)

The comments received broadly agree with the approach proposed by the FSB on proportionality. Some respondents stated that the report should better clarify that the toolkit should be flexible/non-binding. Moreover, it is desirable that Authorities have to apply the proportionality principle when dealing with this topic.

Comments received on identification/designation of service providers as critical (Q14)

Few comments relate to the approaches envisaged by the FSB on the identification of systemic third-party dependency, i.e. the possibility to identify the entire provider as critical. Some comments highlight the value of an enhanced dialogue between supervisors and providers in the identification process. In this regard, a few respondents suggested that financial authorities should communicate to financial institutions which are the providers identified.

Comments received on direct incident reporting (Q15)

The majority of the respondents do not support implementation of the direct reporting by third-party providers to financial authorities. Many respondents noted that financial institutions are well placed to receive, respond, and manage incident notifications from a third-party service provider and report such incidents to financial authorities. Some respondents stated that direct reporting is possible but should only be required for highest level incidents with a potential systemic impact. Respondents suggested that impact thresholds should be established in this case. Many respondents identified challenges they believe make direct reporting ineffective, including that financial institutions are better positioned to provide real-time updates on the impact that any incident would have, and that this would increase regulatory fragmentation with cyber incident reporting (which they note that the FSB has identified as a concern.)

Comments received on challenges and barriers to effective cross border cooperation (Q16) and cross-border information sharing (Q17)

Many respondents pointed to the different regulatory frameworks, including the mandates, legal power such as direct supervisory power over third parties. Some comments referred specifically to the differences in the third-party data collected and the differing methods of identifying critical third-party dependencies. One respondent advocated that any cross-border cooperation be technologically neutral.

The comments detailed the challenges of sharing confidential/sensitive information. One respondent noted that the contractual clauses between the financial institution and the third parties for providing information does not, at least routinely extend to cross border information sharing. Several respondents pointed to the consideration of data security and data governance issues relating to the information sharing. One respondent summed up the obstacles to cross-border information sharing: (1) potential for threat actors obtaining information; (2) confidentiality concerns, and (3) the question of how any cross-border information-sharing is done so that substitutability of information is maintained and addressed, so as not to place unnecessary burdens on financial institutions.

Respondents called for enhanced coordination between different authorities, with many responses pointing to duplication or conflict between differing authorities as potentially, or in actuality, undermining efficiency and resiliency of financial institution's operations.

The majority of respondents supported strengthened cooperation between financial supervisory authorities, including cross-border information sharing as well as testing. In particular, resilience testing was raised as an area where coordination by authorities could be valuable in strengthening financial institutions' and authorities' abilities to identify and address vulnerabilities. Respondents supported the idea of sector-wide and multi-sectoral exercises with respect to internationally active service providers, noting these exercises could build upon evolving testing that institutions and/or third-party service providers already carry out. Respondents also noted value in authorities being able to take into account the results of testing conducted in another jurisdiction or engaging in joint exercises to the extent provided by legal and regulatory authority.

With regards to cross-border information sharing, respondents widely cautioned against oversharing, emphasising the need to carefully consider the level and extent of information shared due to sensitivities, and adequately securing this information. Some respondents noted existing networks to facilitate cross-border coordination or how formal agreements might be leveraged between authorities. A few respondents echoed other challenges noted in the report regarding cooperation, including differences in regulatory and supervisory frameworks. These commenters suggested that efforts surrounding cross-border information sharing could benefit from authorities exploring greater convergence of supervisory approaches, including establishing more similar or consistent information for the identification and assessment of systemic dependencies.

Comments received on forms of cross-border cooperation that authorities should consider (Q18)

Respondents generally approved of the forms of cross-border coordination set forth in the toolkit.

Many respondents noted difficulties in sharing sensitive or commercially protected information cross-border as a hurdle to effective cooperation. One suggested use or modification of Memoranda of Understandings to facilitate this exchange. Another respondent suggested leveraging existing private-public partnerships to overcome sensitive information issues, such as use of CMORG, ECRB, FSCRF and FSSCC to progress on cross-border collaboration.

Several proposed that regulators work with industry to establish consistent criteria and methodologies for assessing, classifying, and identifying systemic third-party dependencies and potential systemic risks. One respondent suggested that there should at least be a standard framework for what specific information and data components are required by authorities that can be shared cross-border. This could help facilitate the exchange of information and promote more efficient oversight.

Several respondents suggested cross-border resilience exercises. One recommended conducting joint exercises of third (and nth) parties with international reach such as business process outsourcing firms, cloud service providers, and payments services providers, among

others. This resilience testing could include testing for whether third-party providers do continuous monitoring.

3. Possible areas for further development by authorities, financial institutions and service providers

The toolkit for enhancing third-party risk management and oversight provides a foundation to address some of the key challenges that financial institutions and authorities face in the area of third-party risk management and oversight. The toolkit also provides a foundation for financial institutions to strengthen their management of critical services and critical service providers, and also sets out a range of possible tools for authorities to manage systemic third-party dependencies and related systemic risks.

However, some areas explored in this toolkit are highly complex and cannot necessarily be addressed to an appropriate level of depth in a principle-based toolkit. Likewise, industry practices and supervisory expectations in some areas are at an early stage and, in some cases, evolving rapidly. A number of consultation responses also noted the importance of strengthening supervisory cooperation.

The consultation responses indicated that there may therefore be value in authorities, financial institutions and service providers exploring some of these issues in greater depth. These could be explored further by existing and potential future fora, including the potential "additional models for international cooperation and information-sharing" examined in section 4.4 of the toolkit. Some possible areas for further exploration may include:

- Ways to further harmonise the data that authorities collect about financial institutions' third-party dependencies, building on the registers and other tools being developed in certain jurisdictions;
- Further work on potential additional tools to help authorities, financial institutions and service providers monitor and manage supply chain risks in a proportionate, resource-efficient, risk-based manner;
- Ways to build resilience into services where substitutability is not a realistic option;
- Ways to ensure that authorities and financial institutions are informed of incidents at third parties in a comprehensive, timely but proportionate manner, in particular, where the service provider is considered a financial sector critical service provider, or the incident could pose risks to financial stability; and
- Ways for authorities to develop and share a common understanding of systemic third-party dependencies, which could over time evolve in mutual recognition frameworks.