Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities

Bank of Russia responses to consultation

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?***

   Regarding the basic definitions, it is not clear which services provided by third parties fall under the scope of the toolkit.
   It appears that the scope of the toolkit should not be extended to the cases where third-party involvement is required by legislation (for example, annual audit), as well to the following services:
   - customer engagement services, sale of financial services;
   - outstaffing;
   - information services provided to financial market participants for conducting business and (or) making investments;
   - functions that are not usually undertaken by financial market participant itself (cleaning services, buildings and premises maintenance, car maintenance, utilities, etc.).

   In addition, it seems relevant to include in the document an overview of existing regulatory limitations (restrictions) on outsourcing of certain functions (for example, functions of financial institutions' management bodies, internal control and audit, risk management, etc.).

   We also propose to add the definition of the term "incident" (see footnote 29 in the document).

Chapter 2

2. ***Are the scope and general approaches of the toolkit appropriate?***
   We support the scope and general approaches of the toolkit. However, we propose to specify what measures can be introduced by financial authorities to facilitate the enhancement of financial institutions' management of concentration risks on service providers (besides higher expectations on the resilience of the selected services mentioned in Section 2.1).

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

   The focus on the regulatory interoperability is a topical issue and will ensure consistency of approaches for assessing systemic dependence on third-party service providers and managing the third-party risks, including in the context of cross-border provision of services by third parties.

4. ***Is the discussion on proportionality clear?***

   Yes, it is clear. The major advantages of outsourcing are cost optimisation and reducing time spent on the development of new business lines, entering the market or expanding the scale of activities. Thus when applying the principle of proportionality, we propose to take into account that the overall benefits of outsourcing should offset the financial institutions' costs related to managing the third-party risks.

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?***

We support the focus on critical services and critical service providers.

The proposed approach to defining the criticality of functions includes an element of evaluation (it is indicated that the criticality of a service can vary over time, be different depending on the business model of financial institution and the volume of services provided). However, we assume that in general, if a financial institution does not change the field of its activities, certain functions should be defined as critical based on their nature, regardless of the changes in the business model, in the volume of services provided, etc.

Moreover, in defining critical services, the following criterion can also be applied: the possibility of having a significant impact on the fulfilment of financial institutions' obligation to customers or causing significant harm to consumers of services as a result of failures in the activities of organisations related to the provision of services by third parties.

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?***

To ensure the confidence of financial market participants in the quality of services provided by critical service providers, and at the same time not to extend the powers of the financial regulator to such providers, the financial regulator can recognise the provider compliant with the regulatory requirements of another regulatory body (if any), for example, based on the license issued by another regulatory body or inclusion of third-party provider in its register.

The following additional tools can be used by financial institutions and regulators to manage the third-party risks:

- compliance with data protection requirements by third-party providers of information and communication services, including providers of cloud services
- establishing the liability of service providers for violation of the data protection requirements (regarding the data received from financial institutions);
- insurance of the specified liability;
- management of conflicts of interest in the activities of third parties when one service provider provides services to several financial institutions.

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?***

If financial institutions provide data on the third-party service providers involved and the services they provide in a harmonized form, this will help the financial regulators to carry out more complete aggregate analysis of the use of third-party services and quickly adapt their regulatory frameworks to these activities. The form for providing data can consist of a common part for all financial institutions and a special part developed for different segments of the financial market, taking into account the special features of their activities.

The data in financial institutions' registers of third-party service relationships should include information on nth-party service providers (at least for significantly important financial institutions), as the information on concentration on the "final" service provider is important for assessing systemic risks. As the document highlights that these data may be provided by financial institutions based on their assessment of the importance of sub-contractors, it seems important to establish criteria for this assessment in order to unify the approaches of different financial institutions.

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?

Yes, we consider the list of tools and their descriptions to be sufficient.

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?***

Approaches and tools for developing business continuity plans are extensively described in the consultative document.

10. ***How can financial institutions effectively identify and manage concentration and related risks at the individual institution level? Are there any additional tools or effective practices that the toolkit could consider?***

The list of tools for managing concentration risks might be supplemented with proposals on possible methodology for calculating or defining level of concentration of service providers.

Besides, we believe financial institutions might identify and manage concentration risks by comparing their level of concentration on certain service providers with the aggregated level of concentration for all financial institutions calculated by the regulatory authority (if this information is publically available). For instance, financial institutions should take into account whether service provider is considered to be critical for the market when estimating risks of using its services.

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

We propose to supplement the risk management recommendations with recommendation for financial organisations to assess risks of service providers located abroad (in other jurisdiction) by analysing economic, social, political 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?***

The concept is readily understood, the scope is appropriate.

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

We believe proportionality can be achieved by estimating a market share of a certain service provider through a market share of financial institutions that use its services in the context of business activity and critical functions. In addition, thresholds might be differentiated depending on financial institution's capability to manage risks related to outsourcing.

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

A matrix can be used to estimate the impact of third-party service providers on the financial market and to develop supervision measures that take into account the principle of proportionality. Financial authority might use such matrix to rank service providers based on the level of concentration on their services (e.g. "low", "medium" or "critical" level of concentration) and to rank financial institutions that use these services based on their significance for the financial system or its segment (e.g. "low", "medium" or "critical" level of significance). Financial authority should give special attention for the following cases:

Level of significance/ Level of concentration	*Low*	*Medium*	*Critical*
Low			
Medium		*!*	*!!*
Critical		*!!*	*!!!*

15. ***Should direct reporting of incidents by third-party service providers within systemic third-party dependencies to financial authorities be considered? If so, what potential forms could this reporting take?***

    Given the fact that generally financial institution is responsible for such communication, it is reasonable that financial institution should report on incidents.

    Nevertheless, direct and prompt reporting of incidents by service providers to financial authority might be considered if such service provider provides critical services that has systemic impact on its clients' stable activity. However, it might be necessary to confer financial authority with necessary powers. Besides, it seems appropriate to set the conditions for such direct and prompt reporting, stipulating that these reports should contain information only on significant events. Such reports may also include information on cause of the incident, recovery period and possible measures to avoid similar incidents.

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?***

    Differences in mandates of financial regulators (different regulatory powers over service providers and the absence of consistent regulatory and supervisory frameworks on third-party risk management) as well as differences in types and kinds of information they proceed and possess is a significant barrier to effective cross-border information exchange.

    We support the FSB work aimed at facilitating greater convergence of regulatory and supervisory frameworks related to third-party dependencies.

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 believe it is reasonable to use both cross border information sharing among financial authorities and testing of certain service providers in order to detect, monitor and manage risks related to oversight of service providers located abroad (in other jurisdiction). We also propose to include preliminary description of such testing in a final version of the report.

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?***

    Effective information sharing and cross-border cooperation among financial authorities are often impeded by legal constraints. In this regard, setting appropriate MoUs between relevant authorities or explicit inclusion of third-party related information in existing supervisory MoUs seems necessary.

    New forms of information exchange based on innovative technologies (such as DLT) could also be explored in this context.