FSB FINANCIAL STABILITY BOARD

14 June 2021

Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships

Overview of Responses to the Public Consultation

On 9 November 2020, the Financial Stability Board (FSB) published a discussion paper for public consultation on *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*.[1] The discussion paper drew on findings from a survey conducted among FSB members, and identified a number of issues and challenges.[2] To facilitate and inform discussions among authorities (including supervisory and resolution authorities), financial institutions and third parties on how to address the issues identified, the discussion paper invited comments from external stakeholders on:

1. the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships (including risks in sub-contractors and the broader supply chain);

2. possible ways to address these challenges and mitigate related risks, including in a cross-border context; and

3. lessons learnt from COVID-19 relating to outsourcing and third-party relationships.

The public consultation period for the discussion paper ended on 8 January 2021. The FSB received 39 responses from a wide range of stakeholders including banks, insurers, asset managers, financial market infrastructures (FMIs), third-party service providers, industry associations, individuals and public authorities.[3] The FSB also held a virtual outreach meeting in late February 2021 to discuss: evolving industry practices; practical challenges associated with outsourcing and third-party risk management; and potential ways to improve coordination among the relevant stakeholders (i.e. supervisory and resolution authorities, financial institutions and third-party service providers) with a view to enhancing the resilience of financial institutions and the financial system.

---

1 FSB (2020), *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*, 9 November.

2 For example, financial institutions have to ensure that their contractual agreements with third parties grant to them, as well as to supervisory and resolution authorities, appropriate rights to access, audit and obtain information from third parties. These rights can be challenging to negotiate and exercise, particularly in a multi-jurisdictional context. The management of sub-contractors and supply chains is another challenge that was highlighted in the context of financial institutions' response to COVID-19. There is furthermore a common concern about the possibility of systemic risk arising from concentration in the provision of some outsourced and third-party services to financial institutions. These risks may become higher as the number of financial institutions receiving critical services from a given third party increases.

3 The consultation responses that can be made publicly available are published on the FSB's website.

Respondents generally welcomed the discussion paper, which they viewed as a timely and balanced overview of the benefits and challenges relating to the evolving nature of financial institutions' outsourcing and third-party dependencies. Respondents agreed with the challenges and issues identified in the discussion paper, such as: constraints on the rights to access, audit and obtain information from third parties; and concentration risks in the provision of certain critical services that are very difficult to substitute. In addition, treatment of intra-group outsourcing, fragmentation of regulatory, supervisory and industry practices across sectors and borders, restrictive data localisation requirements, cyber and data security, and resource constrains at financial institutions as well as supervisory authorities were highlighted as potential challenges or issues that deserve attention.

To address these challenges or issues, respondents suggested a range of measures that can be categorised into five areas: (i) the development of global standards on outsourcing and third-party risk management; (ii) the adoption of consistent definitions and terminology; (iii) pooled audits, certificates and reports; (iv) dependency mapping and enhanced supervisory oversight; as well as (v) enhanced cross-border cooperation and dialogue with stakeholders.

This note summarises the main issues raised and views expressed in the public consultation, including the virtual outreach meeting (which are not necessarily shared and endorsed by FSB members).

1. Key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships

A range of challenges or issues were highlighted by respondents in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships.

- **Complexity and lack of transparency in financial institutions' third-party relationships (or supply chain of technologies and services provided)**. Respondents noted that outsourcing and third-party relationships, including the chain of sub-contractors (or "nth parties") involved, are complex and lack transparency. As a consequence, it is difficult or impossible for financial institutions to influence third-party service providers' sub-contracting decisions, which makes it very challenging for financial institutions to manage and mitigate supply chain risks. A number of respondents noted that financial institutions as well as supervisory and resolution authorities are currently unable to "map" the entities and activities involved in third parties' supply chain, and appropriately assess the impact of supply chain disruption on financial institutions' resilience. Conversely, a few respondents cautioned against exhaustive mapping of supply chain and/or identification of nth-party risks. These respondents noted that the burden and cost of identifying *all* possible entities or scenarios was likely to disproportionately outweigh its potential benefits, creating barriers to innovation, and subsequently reducing access to financial services.

- **Treatment of intra-group outsourcing**: Some respondents highlighted the importance of treating intra-group outsourcing differently from external outsourcing (or outsourcing to third-party service providers). These respondents noted that, in their view, some risks in intra-group outsourcing can be managed proportionately in practice due to the control

and influence that financial institutions typically have over intra-group service providers. In their view, financial institutions should be able to apply globally consistent policies and risk management frameworks to intra-group outsourcing arrangements.

- **Concentration risk**. Many respondents mentioned that concentration of critical services in the same third-party service provider by financial institutions may create risks to the financial system. These risks become greater if the service or product provided by the relevant third party is difficult to substitute (see also "substitutability" below). In addition, a number of respondents highlighted the inability of financial institutions to monitor systemic concentrations in the provision of third-party services as they do not have access to data on other financial institutions' dependencies on specific third-party service providers. Moreover, some services, including certain "niche" services, are provided by a very small number of third-party service providers, and are therefore by their nature concentrated. According to many of these respondents, identifying, monitoring and managing systemic concentration risk in the provision of third-party services and other interdependencies is beyond the responsibility of individual financial institutions. A number of respondents also cautioned against unduly complex or prescriptive requirements to address concentration risk (e.g. a requirement on financial institutions to use multiple vendors) as they could place a disproportionate burden on institutions' operational capacity.

- **Substitutability**. Financial institutions may not be able to substitute certain technologies or services provided by third-party providers in a cost-efficient and timely manner, and without an undue risk of operational disruption. Such lack of substitutability can limit the negotiating power of financial institutions when entering into contracts with third-party service providers and their subsequent ability to monitor the relevant service or technology. Financial institutions in emerging market and developing economies (EMDEs) may face additional challenges trying to locate alternative or back-up third-party service providers in their jurisdictions, or bringing certain services or technology back in-house. One respondent meanwhile noted the potential unintended consequences of requiring financial institutions to exit certain outsourcing or third party arrangements in times of stress. For instance, if a service provider owns a specific piece of software (e.g. code library) or technology, it may not be possible for a financial institution to bring the relevant service back in-house without costly and significant alterations.

- **Fragmented supervisory and industry practices**. Regulatory and supervisory frameworks on outsourcing have been developed by various national/regional authorities and standard setting bodies. They are often prescriptive, and inconsistent across jurisdictions and sectors, leading to fragmented industry practices and increased compliance costs for internationally-active financial institutions. [Some public authority respondents also noted the need for better coordination among home and host supervisory authorities when assessing the resilience of internationally-active financial institutions' outsourcing and third-party arrangements.] Greater global coordination and harmonisation in regulatory and supervisory expectations on best practices both across border and sectors could be helpful in improving management of risks associated with outsourcing and third-party relationships especially for internationally-active financial institutions. A few respondents also noted the need for better coordination among

supervisory authorities when assessing the resilience of financial institutions' outsourcing and third-party arrangements.

- **Data localisation requirements**. A number of respondents raised concerns about stringent data localisation rules in some jurisdictions, or other requirements limiting or prohibiting the flow of non-public data across borders and the use of geographically diversified third-parties, which can undermine, rather than enhance, the operational resilience of financial institutions. In particular, their ability to withstand, respond to and recover from operational disruption can be affected by these restrictive data requirements. These restrictive requirements can also limit the effectiveness of cross-border data management by financial institutions, stifle innovation and increase the costs of outsourcing and third-party arrangements. A few respondents noted that these requirements often stem from the need for authorities to meet certain regulatory objectives, such as ensuring that third-party service providers operating in multiple jurisdictions continue providing or supporting critical services in the event of a financial institution's resolution. However, these respondents suggested that there may be more proportionate ways of achieving these objectives, such as improved coordination among resolution authorities.

- **Cyber and data security**. The quality of the services delivered by a third-party provider (e.g. cloud service provider) is dependent on its ability to appropriately protect the confidentiality, integrity and availability of the data as well as the security and reliability of the systems used to process, transfer or store this data. Ensuring cyber security and an appropriate level of data protection is a challenge for financial institutions as well as for third-party service providers. Some respondents noted that reliance on some services provided by third-parties (e.g. cloud services) can enhance the cyber security of financial institutions relative to their on premise information and communications technology (ICT) infrastructure.

- **Constraints in the relevant resources and skills**. A number of respondents highlighted the scarcity of individuals with specialist skills (e.g. cloud computing and other fast-moving forms of ICT), at financial institutions as well as at supervisory authorities as a practical challenge. Such constrains may limit financial institutions' ability to oversee their third-party relationships and manage the risks associated with new technologies or services they may obtain from third-party providers.

2. Possible ways to address key challenges and associated risks, including cross-border challenges

Respondents suggested possible ways to address the challenges or issues identified in Section1.

2.1. Global standards on outsourcing and third-party risk management

Many respondents recommended *actionable global standards on financial institutions' outsourcing and third-party relationships*. In their view, global standards could strengthen financial institutions' resilience and their ability to manage outsourcing and third-party risks. They could also help to address regulatory and supervisory fragmentation. Greater consistency of

regulatory requirements across sectors and jurisdictions could help to reduce the compliance burden and costs for third-parties and financial institutions.

However, respondents stressed that global standards should be proportionate to the complexity, size, nature and risk profile of different financial institutions. For example, some respondents suggested that standards (e.g. on due diligence) should apply differently to intra-group arrangements as they pose different risks than arrangements with external third-parties.

Respondents also noted that global standards, which could include both regulatory and/or industry standards, should be principles-based, outcomes-focused and proportionate to the criticality of the functions, services or technologies provided or supported by third parties, for financial institutions and the financial system as a whole. Global standards should avoid imposing unduly prescriptive obligations on financial institutions, as this may compromise their efficiency and resilience. Respondents also noted that global standards should be flexible and future proof so that they can adapt to rapidly evolving industry practices and new technologies.

Global standards could address areas such as third-party service providers' business continuity, and disaster recovery plans; financial resilience; ICT security; supply chain management and the provision of information to financial institutions and supervisory authorities in an efficient and timely manner. The standards could also set out expectations for financial institutions relating to their due diligence, monitoring and termination of their contractual arrangements with third parties where appropriate.

Furthermore, a number of respondents emphasised the importance of *standardisation or defining an internationally uniform set of key information that should be collected from third-party service providers* to assist financial institutions' risk management processes and support supervisory authorities' assessment of firm-specific and any potentially systemic risks.

In addition, a few respondents indicated that a *"master agreement" or "model clauses"* could help financial institutions' contract negotiations with third-party service providers.

While recognising the merits of reducing costs of complying with fragmented regulations, a few respondents suggested that regulators should be mindful of the one-off costs of changing existing regulation, especially if the changes are not coordinated.

2.2. Consistent definitions and terminology

A number of respondents asked the FSB to *clarify or improve existing definitions, including terms such as "outsourcing" and "third-party relationships"*, *and criteria for "criticality/essentiality/materiality"* so as to clearly understand what activities are in scope of regulation. For example, some respondents argued that custody services or services provided by FMIs fall outside the definition of "outsourcing".[4] There were mixed views on the treatment of cloud services providers. One respondent suggested different regulation should be applied to cloud service providers as they pose unique challenges, while some other respondents

[4] One respondent meanwhile stated that FMIs are included within the regulatory regime for outsourcing and/or third-party relationships in some jurisdictions.

suggested that arrangements with cloud service providers should not be distinguished from other forms of outsourcing as they share common features.

Some respondents suggested that the FSB should establish *globally consistent definitions and terminology (or a lexicon) related to outsourcing, cloud computing and operational resilience*. Such globally consistent definitions and terminology would help financial institutions to manage risks on a firm/group-wide basis (i.e. across jurisdictions and sectors). It will also help align supervisory and industry expectations. Relatedly, one respondent suggested it would be beneficial for the FSB to develop a global taxonomy for incident reporting.

2.3. Pooled audits, certificates and reports

Many respondents suggested that the FSB should encourage *the use of pooled audits* (collaborative assessments of common third-parties carried out by groups of financial institutions or experts appointed on their behalf) as an effective form of third-party risk management that can help to reduce the burden on the relevant stakeholders, including the burden, costs and potential disruption of multiple financial institutions carrying out separate individual assessments of their common third parties. Pooled audits are already recognised by supervisory authorities and carried out by financial institutions in a number of jurisdictions. A number of respondents did, however, caution that in order for pooled audits to be effective and workable in practice, they would also need to address issues in areas such as anti-trust/competition, confidentiality and data-sharing restrictions.

Some respondents suggested that supervisory authorities should encourage the use of certificates and reports provided by third-party service providers' evidencing compliance with internationally-recognised standards as a means of promoting a consistent approach to third-party oversight by financial institutions. Examples of relevant standards are those issued by the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), Statement on Standards for Attestation Engagements 18 (SSAE 18), System and Organization Controls (SOC 2) or Shared Assessments Standard (SIG). Certificates and reports could facilitate financial institutions' due diligence and their ability to compare the control environment of different third-party service providers. However, the use of certificates and reports should not relieve financial institutions from their accountability for any activities, functions, products or services which they outsource or delegate to third parties.

2.4. Dependency mapping and enhanced supervisory oversight

Several public authority respondents suggested that financial institutions should: *establish an inventory of services and technologies provided by third-parties (including key entities involved in their supply chains) to map financial institutions' dependency on third-parties*; *periodically evaluate the information they receive from third-party service providers*; *regularly update the skills and training of employees responsible for monitoring their third-party dependencies*; and *share their experiences with supervisory authorities*.

A few respondents emphasised the need to enhance existing regulatory and supervisory approaches. For example, by giving supervisory authorities direct access to data, information and at the premises of third-party service providers, and/or enabling them to supervise third-party

service providers meeting certain criteria, such as concentration. One respondent did, however, challenge the effectiveness of on-site supervisory inspections based on their experience. Another respondent stated that in order to directly provide data about its financial institution clients to supervisory authorities, a third-party service provider typically requires the consent or involvement of these financial institutions as clients ultimately maintain control over their data. Thus, in the absence of legal powers or contractual arrangements giving supervisory authorities direct recourse to third parties, the best course of action for supervisors seeking to get access to readable and specific data sets might be to request these data sets from financial institutions.

One respondent noted that regulators had different risk tolerances on financial institutions' approaches to outsourcing, and that different notification and approval timelines can impact their ability to manage resilience. They challenged the requirement for lengthy approval timelines and instead suggested notification would be more proportional, while enhancing dependency mapping.

Some respondents suggested that oversight of third-party service providers that are already subject to financial regulation and supervision (e.g. financial institutions providing custody services and FMIs) should be led by their "home" authority. Other authorities should enter into information-sharing arrangement with the home authority to obtain appropriate information on relevant third-parties.

The *adoption of real time analytics and RegTech/SupTech solutions* to support supervisors and *capacity building at supervisory authorities* will also be helpful.

2.5. Enhanced cross-border cooperation and dialogue among stakeholders

In addition to the development of global standards to manage the risks of outsourcing and third-party relationships, many respondents suggested that the FSB should *organise a regular international forum (or a public-private global working group) comprising relevant stakeholders (i.e. supervisory authorities, financial institutions, third-party service providers) to exchange views and best practices* with a focus on cross-border issues associated with outsourcing and third-party relationships. Such forum could also confidentially discuss concerns and practical experiences on specific cross-border or cross-sectoral issues leveraging on existing regulatory and supervisory arrangements (e.g. supervisory colleges). It could be organised to include researchers and technical experts. It was also suggested that such a forum or working group could map sector-wide third-party dependencies or develop system-wide stress testing scenarios.

Some respondents also suggested enhanced information-sharing among authorities with regard to national/regional regulations (including bank secrecy, data privacy, cross-border data flow rules), guidelines and other supervisory practices. International supervisory training would also be helpful.

3. Lessons learnt from COVID-19 crisis

Most respondents did not mention significant issues with regard to financial institutions' outsourcing or third-party relationships during the COVID-19 crisis.[5] Some stated that the crisis had highlighted the benefits of outsourcing (including cloud outsourcing) relative to: operating all functions "in-house"; accelerated the digitalisation and adoption of digital technologies across the financial services sector; and, in some jurisdictions, promoted financial inclusion through offering financial services online. A number of respondents also stated that the crisis evidenced the resilience of critical service providers (e.g. cloud service providers) and their cyber security capabilities, which they will continue to proactively enhance.

However, respondents also recognised that the crisis had increased financial institutions' dependence on technologies and services provided by third-parties, which highlighted the importance of incorporating risks associated with outsourcing and third-party relationships within the scope of financial institutions' overall (firm-wide) business continuity plans and risk management frameworks. For example, business continuity plans and exit plans could be strengthened and address the recovery from an outage or failure at a third-party service provider and, if necessary, exit the arrangements in a way that minimises potential disruption (e.g. back-up provider, geographical diversification of service providers, planning for longer-term and not for shorter-term impact events). A robust governance around third-party service providers (including asking them to outline the capabilities and oversight of sub-contractors) was also highlighted as important by few respondents. Cyber security also needs to be enhanced as financial institutions increase their dependence on third-party service providers and remote working continues.

A number of respondents noted that the crisis has demonstrated the importance of cooperation and dialogue among relevant stakeholders to respond quickly to events with minimal disruption, although unpredictable incidents or disruptions may still happen despite scenarios and testing have been conducted.

A few public authority respondents observed that the categorisation of critical services at some financial institutions may need to be revisited in light of the crisis. Some services that had been categorised as "not critical" were found to be material. In this regard, analysing the criticality of outsourced services based on different possible scenarios (including for pandemic) should be considered.

[5] Hardware scarcity is an issue faced by some respondents during the COVID-19 crisis.