January 08, 2021

VIA ELECTRONIC SUBMISSION
Financial Stability Board
Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: Discussion Paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

To Whom It May Concern:

The Global Association of Central Counterparties ("CCP12") appreciates the opportunity to comment on the Financial Stability Board's ("FSB") discussion paper on *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships* ("the Discussion Paper").[1]

I. Introduction

CCP12 understands and welcomes the FSB's interest in the topic of regulatory and supervisory issues relating to outsourcing and third-party relationships. Though the paper focuses on financial institutions, CCP12 would like to share the Central Counterparty ("CCP") perspective on this important topic.[2] Before responding to the specific questions in the Discussion Paper, CCP12 would like to make a few general remarks on the issue of outsourcing to third-party provider and draw the FSB's attention to a paper, which was published by CCP12 in July 2019: CCP Best Practices Third-Party Risk Management – a CCP12 Position Paper[3] ("Third-Party Paper"). In this Third-Party Paper, CCP12 elaborates on CCP best practices for effective third-party risk management to reduce risks associated with the operational and commercial benefits that third-party relationships can introduce. Furthermore, the Third-Party Paper is designed to provide a high-level educational tool, and best-practices approach to the industry on vendor risk management practices of CCPs.

[1] FSB, Discussion Paper, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships (Nov. 2020), available at https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/.
[2] This response is not intended to and does not attest to any particular CCP and its individual practice but represents a general consensus view on certain subject matters without prejudicing individual CCP variances. Practices for CCPs' risk management are not "one-size-fits all" and it is important to recognize differences due to market, regulatory environment and other legal matters, ownership structures, operational preferences, and other factors.
[3] CCP12, Position Paper, CCP Best Practices Third-Party Risk Management (Jul. 2019), available at https://ccp12.org/wp-content/uploads/2019/07/CCP_TPRM_Whitepaper.pdf

II. General Remarks:

- Risk arising from outsourcing to a third-party provider, including a cloud service provider, is best addressed with a companywide outsourcing strategy / policy, which allows for an appropriately tailored risk management strategy and adoption of an appropriate governance and oversight framework.

- CCP12 believes that the FSB should explicitly recognise the qualitative differences between a financial institution outsourcing tasks to an unaffiliated third-party and tasks being performed in connection with shared services among affiliates. Importantly, as the FSB notes, the financial institution retains full responsibility, legal liability and accountability to the regulator for all tasks. Therefore, CCP12 would recommend that any final FSB guidance should reflect the difference between a financial institution outsourcing tasks to an unaffiliated third-party and tasks being performed in connection with shared services among affiliates. This is especially pertinent for Financial Market Infrastructures, given the typical combination of regulation across affiliates within a Financial Market Infrastructure group. When tasks are performed as an intragroup service, there is alignment of the interest in the regulated entity in meeting its responsibilities and those performing tasks because the ultimate shareholders are the same. By contrast, when a third-party performs tasks on behalf of a financial institution there may not be such a strong alignment of interests.

- Since mature companies can have hundreds or thousands of third-parties, CCP12 generally agrees with a risk-based approach. CCP12 does not consider that any CCPs outsource critical clearing functions. These risk assessments can be made for each individual third-party or for categories of third-parties. The level of risk will ultimately determine the amount of due diligence that needs to be performed, with high-impact third-parties subject to a more detailed due diligence process. An inherent risk categorization approach would add consistency to initial risk assessments, increase third-party onboarding efficiency, reduce subjectivity to specific third-party assessments, and more importantly, allow the CCP to focus on third-parties that can pose more significant risks to the CCP (i.e. critical vendors). The list below shows a selection of key risk indicators that a CCP may use to assess inherent risk:

    - **Data Risk** - For the CCP to receive the service, does data need to be exchanged with the third-party? If so, what is the data? Could this data include personally identified information (“PII”), CCP financial data, or other confidential or proprietary data? Will the third-party store, transmit, process, generate or access confidential CCP data, networks or systems? Is the third-party capable of abiding by and assisting with data protection requirements?
    - **Operational Risk** - What is the criticality of the good or service to the operations of the CCP? How long can the CCP operate without the third-party, without significant impact?
    - **Geographic Location Risk** - What is the geographic location where the third-party resides and / or operates? Is the country perceived to be a high risk country for corruption?
    - **Physical / Logical Access Risk** - To provide the service, would the third-party require physical or logical access to the CCP? Where / what would the third-party have access to? Could this include any restricted areas or confidential data?

- **Strategic/Reputational Risk** – Is the third-party performing a service that if not completed would impact the CCP? Is the third-party directly interacting with the CCP's clients?
- **Regulatory Risk** - Would any third-party providing this service be required to adhere to any regulatory considerations or obligations? What, if any, impact could this have on availability?
- **Fourth Party Risk** - Does the third-party rely on fourth parties ? Would the third-party's reliance on fourth or further parties impact its ability to provide services to the CCP.

- Concentration risk can be a concern if there is use of the same third-parties across the business. Sector-wide concentration risk issues should be monitored by regulators.

- Fourth party risk is a concern; there is often limited visibility or transparency, as third parties are not always eager to disclose their third or fourth parties and CCPs have to rely on the fact that the third parties have mature vendor management practices and have a good handle on their third parties. While in general, fourth party risk management is important and a 'best practice', this is a discipline that will need to continue to evolve.

We stress that in our specific answers below, many of the concerns may not arise, or are mitigated in practice, depending on the status and licensing of the third-party or outsourcing provider. For instance, if a CCP uses a third-party, which is a regulated Financial Market Infrastructure, then many of the potential risks are addressed through the supervision of the other Financial Market Infrastructure itself.

III. Responses to Specific Questions in the Discussion Paper

Q1. What do you consider 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?

CCP12 broadly agrees with the regulatory and supervisory challenges and risks identified in the FSB Discussion Paper:

(i) Practical challenges, including supply chain management (i.e. sub-contractors/outsourcing);
(ii) Cross-border challenges; and
(iii) Potential systemic risk (i.e. concentration risk).

Sub-outsourcing:
CCP12 agrees with FSB's assessment that sub-outsourcing and broader supply chain are a potential risk which need to be addressed. Nevertheless, CCP12 would like to point out that in many cases financial institutions have limited visibility, and limited ability to increase visibility, on the sub-outsourcing, especially in the case of indirect outsourcing (i.e. where third-party provider sub-contracts). However, CCP12 believes that a CCP should define the service levels with the service provider and expect those to be met by them regardless whether there is sub-outsourcing or not.

Cross-border challenges:
Cross-border business tends to lead to cross-border challenges for financial institutions as well as regulators and supervisors alike. While some challenges and risks related to outsourcing and third-party relationships are certainly new and different, some are similar to challenges and risks arising out of any cross-border business. Hence, CCP12 believes that proven methods of successful collaboration between regulators and supervisors for cross-border supervision should be the starting point. More specifically, CCP12 implores regulators and supervisors to abide by the principle of mutual regulatory deference by appropriately recognizing the local regulatory requirements applied to CCPs in the jurisdiction for which they are domcilied. This forms the foundation of the G20's committments and in turn, allows local policy-makers to adopt requirements that are appropriate for the markets they oversee and the institutions they regulate and supervise.[4] To that end, CCP12 welcomes the ongoing work at international level, such as the Discussion Paper and IOSCO's work on principles on outsourcing[5]. These international coordination efforts will help to guide discussions at national level and should avoid regulatory and supervisory overlaps or gaps.

Concentration risk:
The Discussion Paper rightly identifies concentration risks as one of the critical issues within the relationship between financial institutions and third-party providers. However, it will be difficult for an

[4] Group of 20, Leaders' Statement, Pittsburgh Summit (Sept. 2009), *available at* https://www.fsb.org/wp-content/uploads/g20_leaders_declaration_pittsburgh_2009.pdf; Group of 20, Leaders' Declaration, Saint Petersburg Summit (Sept. 2013), *available at* https://www.fsb.org/wp-content/uploads/g20_leaders_declaration_saint_petersburg_2013.pdf.
[5] IOSCO, Consultation, IOSCO consults on outsourcing principles to ensure operational resilience (May 2020), available at https://www.iosco.org/news/pdf/IOSCONEWS567.pdf

individual financial institution to assess the concentration risk within a sector. Financial institutions will not have visibility to the outsourcing arrangements of competitors in the same sector or the wider industry. Concentration can only be properly assessed and addressed by regulators and supervisors, who have an overview of the whole market. A CCP should not be penalized/or limited in their freedom to contract just because of concentration risk i.e. a CCP should not be prohibited to outsource to a specific service provider due concentration risks alone, if the relevant service provider is the only one / best one to be providing this service. Ideally, the focus should be on the CCP having effective resilience to issues that the CCP may be exposed to as a result of outsourcing, thus mitigating the impact of concentration risk. Limiting the freedom to contract would have unintended consequences of distorting or limiting competition among the firms that wish to provide the outsourced services.

Q2. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?

Governance and Oversight Framework: CCP12 believes that financial institutions should consider the following best practices when developing a governance and oversight framework for managing outsourcing / third-party relationships:

- A outsourcing governance and oversight framework should:
  - differentiate between outsourcing on a risk-based approach (we do not consider that any CCPs outsource critical clearing functions); and
  - include a risk analysis/assessment.
- Pre-outsourcing analysis and due diligence should be performed before the conclusion of an outsourcing agreement and ongoing third-party performance should be monitored.
- The financial institution should enter a legally binding written contract with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task. The written agreement should specify the rights and obligations with respect to reporting, access, performance levels, inspection and auditing, which should be proportionate to the risk involved and the size and complexity of the outsourced activity.
- The financial institution and the third-party provider should take appropriate steps to make sure both the financial institution and third-party establish procedures and controls to protect the financial institution's proprietary and client-related information and software, and to ensure continuity of service to the financial institution, including a plan for disaster recovery with periodic testing of backup facilities.
- Having a framework in place to discuss amending existing arrangement with the service provider due to regulatory requirements may be sensible and reasonable. However, it is uncertain whether it can be reasonably expected that a service provider would contractually commit to address any unknown regulatory changes.
- Furthermore, the financial institution should clearly specify relevant rights and obligations, include written provisions relating to the termination of outsourced tasks in its contract with service providers, and maintain appropriate exit strategies.

This approach allows for a proportional risk-based approach, which considers the financial institution's business models.

Sub-contractors: CCP12 agrees with the FSB's assessment that sub-outsourcing and broader supply chain are a potential risk which need to be addressed. In order to mitigate the risk if a third-party provider outsources critical or important elements of outsourced critical or important functions a written agreement between the financial institution and the third-party provider should:

- Specify any part or aspect of the outsourced function that are excluded from potential sub-outsourcing;
- Indicate the conditions to be complied with in case of sub-outsourcing;
- Specify that the third-party provider is obliged to oversee those services that it has sub-outsourced to ensure that all contractual obligations between the third-party provider and the financial institution are continuously met;
- Include an obligation for the third-party provider to notify the financial institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the third-party provider to meet its obligations under the outsourcing arrangement with the financial institution. The notification period to be set should allow the firm enough time to carry out a risk assessment of the proposed sub-outsourcing or material changes thereof and to object to or explicitly approve them;
- Grant the financial institution the right to object to the intended sub-outsourcing, or material changes thereof, or that explicit approval is required before the proposed sub-outsourcing or material changes come into effect;
- Grant the financial institution the contractual right to terminate the third-party outsourcing arrangement with the third-party in case it objects to the proposed sub-outsourcing or material changes thereof and in case of undue sub-outsourcing, i.e. where the third-party proceeds with the sub-outsourcing without notifying the firm or it seriously infringes the conditions of the sub-outsourcing specified in the outsourcing agreement.

Exit provisions/strategy: CCP12 supports the idea of having exit provisions/strategies in place for outsourced critical and important functions. To that end financial institutions should consider:

- Including written provisions relating to the termination of outsourced tasks in their contract with service providers; and
- Maintaining appropriate exit strategies (as discussed further below) that includes for example, language contemplating a new service provider and continuation of service until the new service provider takes over the service.

The testing of exit strategies and / having designated secondary service providers on call is a sensible precautionary step for critical outsourced services. As CCPs do not outsource critical clearing functions, the active testing or designation of on-call secondary service providers will not provide substantial benefit that outweighs the commercial and operational challenges, and as such CCP12 would highlight that for CCPs, there should not be prescriptive requirements for across-the-board testing and on-call alternate service providers.

As already explained above, CCP12 sees a qualitative difference between a financial institution outsourcing tasks to an unaffiliated third-party and tasks being performed as an intragroup service among affiliates. When tasks are performed as an intragroup service, there is alignment of the interest in the financial institution in meeting its responsibilities and those performing tasks because the ultimate shareholders are the same. Therefore, CCP12 believes that this difference should also be recognized by regulators and supervisors when assessing outsourcing and third-party relationships.

Q3. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?

Collaboration between financial institutions, third-party service providers and supervisory authorities is key to address cross-border challenges. To that end, CCP12 welcomes the ongoing work at international level, such as the Discussion Paper and IOSCO's work on principles on outsourcing[6]. These international coordination efforts will help to guide discussions at national level and hopefully avoid regulatory and supervisory overlaps or gaps. As above, CCP12 implores regulators and supervisors to abide by the principle of mutual regulatory deference by appropriately recognizing the local regulatory requirements applied to CCPs in the jurisdiction for which they are domiciled.

Further, exchange of industry best practices between financial institutions, third-party service providers and supervisory authorities will contribute to a better understanding of the relevant processes and policy on how to better manage cross-border outsourcing and third-party relationship. To that end, CCP12 would like to once again draw FSB's attention to a paper, which was published by CCP12 in July 2019: CCP Best Practices Third-Party Risk Management – a CCP12 Position Paper[7]. In this paper, CCP12 elaborates on CCP best practices for effective third-party risk management, which are intended to reduce risks associated with the operational and commercial benefits that third-party relationships can bring. Furthermore, the paper is designed to provide a high-level educational tool, and best-practices approach to the industry on vendor risk management practices of CCPs.

Importantly, the financial institution retains full responsibility, legal liability and accountability to the regulator for all tasks; hence CCP12 would like to stress that in case of questions about outsourcing and third-party relationship, the supervisory authority should by default first contact the financial institution. The financial institution should deliver information to its primary supervisory authority based on information obtained via requests from the outsourcing service provider.

[6] IOSCO, Consultation, IOSCO consults on outsourcing principles to ensure operational resilience (May 2020), available at https://www.iosco.org/news/pdf/IOSCONEWS567.pdf

[7] CCP12, Position Paper, CCP Best Practices Third-Party Risk Management (Jul. 2019), available at https://ccp12.org/wp-content/uploads/2019/07/CCP_TPRM_Whitepaper.pdf

Q4. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

The COVID-19 pandemic reinforced the need for service providers to be able to provide an unaffected service during business continuity events, such as remote working capacity. Moreover, service providers' remote working practices and procedures need to maintain the protection of non-public (e.g. client-related) information. The importance of preserving confidentiality could be highlights in a written contract to make sure the service provider protects confidential material in all circumstancings, including business continuity measures or strategies. finally, the third-party provider should offer and guaranty the same level of access control, redundancy systems and Cyber Security regardless of the location of the staff i.e. working onsite vs. working remote.

IV. About CCP12

CCP12 is the global association for CCPs, representing 37 members who operate more than 60 individual central counterparties (CCPs) globally across the Americas, EMEA and the Asia-Pacific region.

CCP12 promotes effective, practical and appropriate risk management and operational standards for CCPs to ensure the safety and efficiency of the financial markets it represents. CCP12 leads and assesses global regulatory and industry initiatives that concern CCPs to form consensus views, while also actively engaging with regulatory agencies and industry constituents through consultation responses, forum discussions and position papers.

For more information please contact the office by e-mail at office@ccp12global.com or through our website by visiting ccp12.org.

V. CCP12 Members