July 14, 2022

VIA ELECTRONIC SUBMISSION (FMIFeedback@bankofengland.co.uk)
Bank of England
Outsourcing and third-party risk management consultation papers (CCPs)
Financial Market Infrastructure Directorate
Bank of England
20 Moorgate
London EC2R 6DA
United Kingdom

Re: CCP12 response to Bank's Consultation Paper on Outsourcing and third-party risk management: Central Counterparties

The Global Association of Central Counterparties ("CCP12") appreciates the opportunity to comment on the Bank of England's ("Bank") Consultation Paper on Outsourcing and third-party risk management: Central Counterparties ("Consultation").[1]

CCP12 is the global association for central counterparties ("CCPs"), representing 40 members who operate over 60 individual CCPs globally across the Americas, EMEA and the Asia-Pacific region.

In addition to this response, CCP12 and its members remain at the service of the Bank for further conversations and provide any further information that may be useful.

CCP12 understands the Bank's interest in the topic of outsourcing and third-party risk management and would like to draw the Bank's attention to its 2019 paper, CCP Best Practices Third Party Risk Management – a CCP12 Position Paper[2] ("Third-Party Paper"). In this Third-Party Paper, CCP12 elaborates on CCP best practices for effective third-party risk management to reduce risks and balance the operational and commercial benefits of these third-party relationships. Furthermore, the Third-Party Paper is designed to provide a high-level educational tool, and best-practices approach to the industry on CCP third-party management practices.

[1] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link
[2] CCP12, Position Paper, CCP Best Practices Third Party Risk Management – a CCP12 Position Paper (Jul. 2019), available at Link

We, furthermore, would like to reference CCP12's response[3] to the FSB Discussion Paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third Party Relationships[4], which includes CCP12's view on the challenges to identify, manage and mitigate the risks relating to outsourcing and third party relationships, how the challenges can be addressed and related risks mitigated and possible ways on how financial institutions, third party service providers and supervisory authorities can collaborate to address these challenges on a cross-border basis.

I. CCP12 Comments on Chapter 1: Introduction

CCP12 appreciates the Bank's efforts to consider international standards relating to third party relationships and outsourcing[5]. However, we would see the need to also include the International Organisation of Securities Commissions' ("IOSCO") Principles on Outsourcing to table 1 "Existing expectations on outsourcing and third-party risk management for CCPs"[6] as these include principles that guide how CCPs, and other Financial Market Infrastructures ("FMIs") manage this risk and to align the Consultation with international existing principles.

Broadly, CCP12 appreciates the principles-based approach that international standards have embraced in many cases, like *Principles for financial market infrastructures* (April 2012) ("PFMIs")[7], which enables CCPs to manage risks effectively and efficiently. Consequently, we are concerned with the highly detailed nature of the Consultation. A CCP's risk management practices, including its approach to outsourcing and third-party risk management, are dependent on the unique characteristics of a CCP's offering. A CCP must be able to design its approach to outsourcing and third-party risk management specific to the structure of the CCP and type and level of services provided by the third party. Highly detailed requirements, as proposed in the Consultation, could unintentionally undermine the ability of a CCP to manage its outsourcing arrangements and third-party risks most effectively. This result would run contrary to the Bank's objective that '*CCPs should thoroughly identify, assess, measure, monitor, and control the risks associated with their third parties to within Board approved risk appetite*'[8], which we fulsomely support.

Along these lines, CCP12 observes that the Consultation, including the draft SS, puts a significant amount of focus on cloud service providers and the use of them, despite the fact that concentration is not unique to cloud service providers. While CCPs are fully aware of the importance of managing the risks arising from the use of cloud service providers (should a CCP use them) similar to other third parties, we believe assessing cloud service providers in a separate category from other third parties is unwarranted. A CCP's

[3] CCP12, Response, FSB Discussion Paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third Party Relationships (Jan. 2021), available at Link
[4] FSB, Discussion Paper, Regulatory and Supervisory Issues Relating to Outsourcing and Third Party Relationships (Nov. 2020), available at Link
[5] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 19 section 1.6
[6] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 19 table 1
[7] CPSS – IOSCO, Principles, Principles for financial market infrastructures (Apr. 2012), available at Link
[8] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 26 section 4.6

third party risk management framework and its related practices are designed to allow a CCP to assess, monitor, and control the unique risks associated with the various types of third parties it may face and it is of the utmost importance that CCPs maintain the necessary flexibility to manage the relationships with disparate types of third parties for which they engage (e.g., IT providers (for the cloud or risk systems), general consulting, data vendors, legal and regulatory reporting). The Consultation appears to put an emphasis on concentration risk, but it's important to note that concentration risk is one example of an important risk that is already monitored and managed through existing CCP frameworks and practices. Risks to third parties must be managed holistically – e.g., avoiding concentration risk could come at the cost of inappropriate security and compliance risks. Similarly, for any given third party of a CCP, including cloud service providers, it is well understood that both the CCP and the given third party must understand their respective responsibilities, including with respect to data protection where that is a relevant factor. Broadly, the risks borne by cloud service providers can be and are already effectively managed within a CCP's current third-party risk management practices (e.g., some CCPs already use cloud service providers today) and unique treatment is unnecessary. This fact should be reflected in the SS. CCP12 also includes more specific comments relating to cloud service providers in the sections that follow.

Finally, as a general point, CCP12 would like to stress that CCPs cannot control how many providers there are, or how their competitors/peers use these services.

II. CCP12 Comments on Chapter 2: Definitions and scope

Notwithstanding CCP12's support for a principle-based approach, as detailed above, to the extent a more prescriptive approach is taken, CCP12 notes that in the Section 2.1[9], the terms "important business services" and "impact tolerances", are not defined in the text and thus, to avoid misinterpretation and align with existing requirements, we would recommend the Bank to include a definition or a reference to the Bank Prudential Regulation Authority's ("PRA") published Policy Statement PS6/21 "Operational resilience: Impact tolerances for important business services"[10].

Furthermore, to align the definition of "outsourcing arrangements" in the Consultation to other international guidelines such as the European Banking Authority's ("EBA") "Guidelines on Outsourcing arrangements"[11], CCP12 recommends the Bank to amend its definition to read as: "[…] an arrangement of any form between a CCP, and a third party, whether a supervised entity or not, by which that third party provides a product, performs a process, a service, an activity or a business function, whether directly or by sub-outsourcing, which **reasonably** would otherwise be undertaken by the CCP itself."[12]

[9] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 20 section 2.1
[10] Bank PRA, Policy Statement, PS6/21: Operational resilience: Impact tolerances for important business services (Mar 2021), available at Link
[11] EBA, Final Report, EBA Guidelines on outsourcing arrangements (Feb 2019), available at Link
[12] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 20 section 2.2

III. CCP12 Comments on Chapter 3: Proportionality

Generally, CCP12 supports the Bank's proposed proportional approach under the Consultation, as well as an approach that considers the criticality (or lack thereof) of an outsourcing arrangement. We believe proportionality and a criticality assessment would work cohesively with the benefits of embracing principles-based regulations that allow CCPs to tailor their risk management practices to the unique characteristics of their practices, as described above.

CCP12 believes that a differentiation needs to be drawn as to the risk of affiliated vendors vs. third parties. The risk profile of intragroup arrangements is much different than that of an organization that sits outside of the institutional protection scheme and the Consultation should recognize these differences. As an example, creating exit strategies for intragroup IT/cyber relationships may not be the best area to prioritize for an organization. Exiting intragroup IT relationships would affect other intragroup services that rely on these services to function. Further, the exiting of these services to external third parties may increase the organization's operational risks or may not be financially feasible for the CCP.

IV. CCP12 Comments on Chapter 4: Governance and record-keeping

As a general remark, CCP12 would highlight possible confusion which may arise from the use of the term "Board" across different jurisdictional conventions. In some cases, "Board" is understood to form a higher level governance body that is composed primarily of individuals serving multiple part-time functions across various institutions, and in others it is intended to capture the key roles of CEO, CRO, CFO, CIO, etc., of management of the CCP itself. To avoid misunderstandings, and to add context to our more precise comments, CCP12 would note that the PFMIs capture these nuances carefully and would strive to maintain this considered language across regulatory work across the globe.

It is important to acknowledge that a CCP's Board and senior management have separate roles when managing a CCP's third-party risks. When these roles are intertwined, it may create confusion on the roles each body plays in the CCP's risk management implementation, as well as undermining the careful check and balance relationship a CCP's Board and senior management maintain. Regarding the Bank's statement that '*boards and senior management cannot outsource their responsibilities*'[13], it is of the utmost importance that it is clearly recognized that the CCP's Board and senior management cannot outsource their accountability, but they do and should have the ability to, outsource their direct responsibility to conduct the day-to-day work (e.g., use of a third party auditor to provide its analysis of books and records and adequacy of the organization's cybersecurity control environment). Consistent with the PFMIs (i.e., Principle 2) and corporate governance principles, in order for the Board to act as an effective check and balance on those individuals performing the day-to-day responsibilities for managing third party risks, it must not engage in the day-to-day risk management at the CCP.

[13] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 25 section 4.3

As such, we would draw attention to our unease with Appendix 4.4 bullet 2 and that the Board should '*bear responsibility for the effective management of all risks to which the CCP is exposed* […]'[14]. The Board is responsible for oversight and senior management is responsible for execution. Therefore, senior management would be responsible for the effective management and the Board would be responsible for approving the CCP's risk appetite and risk management framework and providing effective challenge for the material risks presented to the CCP. Furthermore, the senior management would be responsible for identifying a CCP's critical third parties and managing the risk of those third parties in line with the risk appetite approved by the Board.

Along these lines, CCP12 agrees with the Bank that a CCP should have the flexibility to determine the person to assign responsibility for third party risk and outsourcing.[15] Generally, we believe as a matter of best practice, the responsibility for the third-party risk management framework, policy, systems, and controls should not belong to a member of the Board but instead to a senior executive. This would appropriately preserve the check and balance between the board and individuals responsible for the day-to-day risk management of the CCP. CCP12 notes that in some smaller organizations, this may not be the case.

CCP12 also agrees that the Board should review, understand, and approve the frameworks that are used by the CCP to manage third party and outsourcing risks.[16] In line with the above, the senior management is responsible for the implementation of the third-party risk management practices. Furthermore, we believe the frequency of the regular review of this framework is unclear in the Consultation Paper, thus CCP12 believes that it should be clearly stated that regular review would be satisfied by biennial review.

We have some concerns, as outlined below, with the Bank's proposal in the Consultation (Appendix 4.16) that *'CCPs should make outsourced and third parties aware of relevant internal policies, including those on outsourcing, data protection, information technology, cyber security, and operational resilience. Where CCP policies include confidential or sensitive information, CCPs should omit or redact it and only share those sections relevant to the performance of the outsourced or third-party service.'* Regarding the information to be provided to third parties (e.g., all relevant internal policies), CCP12 recommends that the focus be on only providing them with the salient requirements to the relationship in question, despite CCP's third parties being contractually obligated for the secure management, processing, and destruction of its information in line with the CCP's policies and standards. CCP policies and standards are also often considered confidential information. Sharing policies and standards could create heightened risk due to the concentration of this information at the third party. Further, while providing redacted documents, as suggested in the Consultation, may provide the third party with the given CCP's policies, there may be instances where the redacted document becomes unreadable or otherwise distorts the requirements, thus rendering the information inadequate. CCP12 recommends that the Bank allow alternate means (e.g., policy/standard summaries) to communicate risk and control requirements to these third parties and outsourcing entities.

[14] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 25 section 4.4
[15] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 27 section 4.13
[16] Bank, Consultation Paper, Outsourcing and third party risk management: Central Counterparties (May 2022), available at Link, page 28 section 4.15

Further, we have some concerns, as outlined below, with the Bank's proposal in the Consultation (Appendix 4.17) that *'CCPs should also set out their policy and communicate their expectations (e.g., as part of the scheme rules or their rulebook) when participants engage in outsourcing arrangements that may create new risks to clearing services, or amplify existing risks. CCPs should set out in their policy how the risks to clearing services may be mitigated. For example, when participants are permitted to outsource their connectivity to financial market infrastructure to the cloud, the safety, efficiency, and operational resilience of clearing services may be dependent on the relevant CSPs'.* Regarding this, notwithstanding our broader comments about the focus given to cloud service providers, as outlined in Section I, cloud implementations vary by implementation between the cloud service provider and participant based on the design of the application and the shared responsibilities model between the cloud service provider and participant. Therefore, the participant and cloud service provider would be best positioned to identify the security requirements that should be in place to best secure the network environment. Further, CCPs commonly point to industry-accepted security standards for the protection requirements instead of attempting to develop separate security standards. This ensures that a consistent and proven approach to security is taken when securing the environment used to connect to CCP services.

V. CCP12 Comments on Chapter 5: Pre-outsourcing phase

CCPs have well-defined risk governance processes that are used to manage the risks it faces, including through use of third-party providers, which typically include preferred contract provisions. We believe the proposals in the Consultation undermine these processes, particularly the proposal (Appendix 5.10) that '*The Bank expects CCPs to notify the Bank and seek the Bank's non-objection when entering, or significantly changing a critical outsourcing or third-party arrangement.*' It further reads, '…[T]*he Bank also expects CCPs to submit these notifications before an outsourcing arrangement that was not initially deemed critical is expected or planned to become so'.*

Regarding the non-objection process proposed, especially as it applies to "entering" into an arrangement, we believe this undermines the responsibility and ability of the CCP to make decisions with respect to the third parties it engages, while substituting the judgment of the Bank for the judgment of the entities managing risk in the markets they clear. We of course assume that the Bank would continue to maintain supervisory oversight of a CCP's risk governance processes, but this no objection process would constitute a dramatically different ex-ante responsibility for the Bank to determine and manage the third parties for which a CCP may engage. The proposed non-objection process would be akin to the Bank determining if a given entity should be permitted to be a clearing member of a CCP, which would be highly inappropriate.

There are also certain types of externalities that may create a change in a CCP's risk profile. These events could be geopolitical (e.g., armed conflict); changes to the tactics, techniques and procedures used by cyber threat actors (e.g., increased use of Ransomware); or the identification of a new critical software vulnerability impacting numerous business technologies (e.g., Log4J). In these scenarios, it is unclear how a non-objection may impact the CCP as the CCP has no control over these events.

Additionally, requesting the receipt of a non-objection may create delays in the contractual process and services implementation due to delayed supervisory response, create lack of certainty on the basis it is for a non-objection, or could inappropriately result in a re-negotiation of contractual terms[17]. For the above-mentioned reasons, CCP12 is significantly concerned and strongly disagrees with the proposal that CCPs seek a prior non-objection from the Bank before outsourcing a service as described in Appendix 5.10.

Furthermore, we are generally concerned with the proposals included in Appendix 5.11. In particular, requiring CCPs to inform the Bank of material changes to their risk profile, which may include a participant's use of cloud services to connect to the CCP is hardly feasible considering that it may be participants' chosen means of access based on their risk assessments to connect to the CCP.

In reference to Appendix 5.16 and 5.19, we would like to emphasize that the ability for an individual CCP to gain insight of the systemic risk from a third party to the overall financial markets or of potential dependencies is limited and therefore we believe this should be amended accordingly. In particular, the Consultation states:

> '[*I*]*n line with PFMI Principle 17 for Operational Risk and UK EMIR RTS 153/2013 Article 18, CCPs should, in a proportionate manner, identify the plausible sources of operational risks. These should include the potential risks arising from dependencies on third parties, regardless of criticality, and mitigate their impact through the use of appropriate systems, policies, procedures and controls. CCPs should also conduct risk analysis to identify how various scenarios affect the continuity of its critical operations. […] As risk managers, the Bank expects CCPs to periodically (re)assess and take reasonable steps to identify and manage: concentration risks or vendor lock-in at the CCP due to: multiple arrangements with the same or closely connected third parties; sub-outsourcing or supply chain dependencies, for instance, where multiple otherwise unconnected third parties depend on the same sub-contractor for the delivery of their services; arrangements with third parties that are difficult or impossible to substitute; concentration of outsourcing and other third party dependencies in a close geographical location, such as one jurisdiction. This type of concentration may arise even if a CCP uses multiple, unconnected third parties, for instance, a business process outsourcing or offshoring hub; and an indirect reliance on other third parties when participants outsource their financial market infrastructure connectivity, including hardware and other solutions, to the cloud. When multiple participants use common third parties, operational risks can be correspondingly concentrated and the third party may become a source of systemic risk.'*

Regarding the above, while CCPs have visibility into their own use of third parties, they do not have knowledge (nor authority to obtain the knowledge) of the use of third parties by other financial institutions and similarly, CCPs may not receive (nor otherwise have access to) the information from its third parties necessary to determine the concentration risk that it would have from its sub-outsourcers. Additionally, as an example, CCPs may offer several connectivity options to its participants, but CCPs cannot limit the

[17] If the Bank requires the CCP to add contractual terms, this could cause the CCP to re-initiate contract negotiations with the third party further elongating the contract process. Contract proposals have a limited timeframe for the terms and costs of services. Delays in the contract negotiation created by the non-objection process may lead to further re-negotiation of contractual clauses.

use of connectivity methods to certain participants. Participants make independent decisions on how connect to a CCP's services, including if they use a cloud service provider and whether multiple connectivity options should be established. While CCPs have visibility into a participant's cloud service provider usage to connect to its services, it does not have a view into other services that the participant may be obtaining from these vendors, nor does it have decision-making authority on the participant's cloud service provider usage. Insights and expected actions for sector-wide concentration risk may best be addressed by the financial authorities. Given these limitations, CCP12 recommends that the Bank modify the text (i.e., at a minimum, Appendix 5.16 and 5.19) to be clear that CCPs -or that via CCPs the Bank is responsible for- are not managing the risk of sector-wide third-party use and concentration risk.

VI. CCP12 Comments on Chapter 6: Outsourcing agreements

We agree with the Consultation's proposal that the agreements between a CCP and third party should be written and clearly define the expected service levels and the terms under which those are met, but ultimately, the terms of those agreements should be determined between the CCP and third party, thus we are concerned with the detailed nature of the proposals in the Consultation (Appendix 6.4). Additionally, the CCP has the legal relationship with the third party and must be able to determine the terms of those relationships and if they are satisfied if those terms fit within its risk appetite. Furthermore, the prescriptive nature of the proposal may not adequately account for the fact that agreements rightfully vary across different types of third parties. Additionally, even though many of the proposed requirements are common practice across CCPs (e.g., a clear description of the outsourced function, the governing law of the agreement, the parties' financial obligations), there could be implementation challenges for some terms proposed.

For example, the Consultation (Appendix 6.4) states that *'Written agreements for critical outsourcing arrangements should set out at least the following: […] the extent to which the provision of each important business service of the CCP are dependent on a third party'.* While CCP12 agrees that third parties should be provided with clear and documented information, including regarding any shared responsibilities, many CCPs do not inform a cloud service provider of the applications or business processes being supported on its infrastructure. CCPs do, however, communicate the risk and resilience controls required for its business processes. Providing application, application data, or supported important business service increases the surface area available to the loss of this information, or more important, could be used by nefarious actors to target specific financial services operations. CCP12 recommends that the Bank consider allowing the current practice of limiting the distribution of this sensitive information to its third parties and that information regarding the service is strictly limited to what the third party needs-to-know to meet the CCP's risk and resilience requirements.

As another example, the Consultation states that '*Written agreements for critical outsourcing arrangements should set out at least the following: […] whether the sub-outsourcing of a function or part thereof is permitted and, if so, under which conditions*;'. While there may be some cases where third parties must request approval for subcontracting material aspects of their service, the more common approach is that third parties must notify its clients of sub-outsourcing. Hence, CCP12 recommends the

Bank not to be specific on the contractual terms regarding sub-outsourcing so as to recognize the different approaches regarding sub-outsourcing. We further detail our views on sub-outsourcing in Section IX.

More broadly, CCPs (and other financial institutions) continue to face challenges when negotiating contractual clauses[18]. CCP12 requests that the Bank consider the ongoing challenges with the negotiation of certain contractual terms (e.g., Right To Audit) and that the list of terms proposed in the Consultation be removed, but at a minimum, it should be recognized that this list is for consideration when entering into agreement and there should be clear recognition of situations where there is limited negotiating power with vendors and these terms cannot all be negotiated. Notably, additional analysis, planning, and the implementation of operational measures (e.g., add resiliency) can take the place of some of these contractual elements if executed correctly.

VII. CCP12 has no comment to Chapter 7: Data security

VIII. CCP12 Comments on Chapter 8: Access, audit, and information rights

CCPs conduct multiple due diligence activities to understand the risk governance and controls in place at its third parties. The breadth of these activities is based on the risks presented by the third party to the CCP's operations.

We have one request with regard to Bank's proposal in the Consultation (Appendix 8.4) that *'CCPs proposals on effective access, audit, and information rights should cover (as appropriate) premises, data, devices, information systems, and networks used for providing the service or monitoring its performance. These should include, where relevant: […] the results of security penetration testing carried out by the outsourced third party on its behalf, on its applications, data, and systems to assess the effectiveness of implemented cyber and internal IT security measures and processes;'.* Regarding the proposal, third parties often do not provide the results of security penetration testing given the sensitivity of the information contained in these results and the increased risk that these results may be lost, stolen, or inappropriately managed by its clients. CCP12 requests that the Bank allows third parties to provide either certificates of completion or testing summaries in lieu of providing the testing results.

Finally, we would stress the importance that for information concerning the CCP itself, that such request go first and foremost to the CCP itself, rather than directly to third parties. This is a natural aspect of information rights, but it crucial to prevent a risk of inappropriate data dissemination.

IX. CCP12 Comments on Chapter 9: Sub-outsourcing

As further described in Section V, CCPs have limited visibility, and limited ability to increase visibility, on the sub-outsourcing. CCP12 believes that a CCP should define its required service levels with the third

[18] FSB, Discussion Paper, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships (Nov. 2020), available at Link, page 12

party and expect those service levels to be met regardless of whether there is further sub-outsourcing of the service. In line with CCP12's comments in Section VI, we echo the Consultation's proposal that it's important that agreements between a CCP and third party are written and well-defined, but ultimately, the terms of those agreements should be determined between the CCP and third party, thus we are concerned with the detailed nature of the proposals in the Consultation (Appendix 9.9). As referenced above, the CCP has the legal relationship with the third party and must be able to determine the terms of those relationships and if they are satisfied if those terms fit within its risk appetite. For these reasons, CCP12 requests that the list of terms proposed in the Consultation be removed, but at a minimum, it should be recognized that this list is for consideration when entering into agreement and there should be clear recognition of situations where there is limited negotiating power with vendors and these terms cannot all be successfully negotiated.

X. CCP12 Comments on Chapter 10: Business continuity and exit plans

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 highlighted in a written contract to make sure the service provider protects confidential material in all circumstances, 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.

Broadly, we appreciate that the Bank does not prescribe or have a preferred form of exit planning for stressed scenarios. Flexibility in this respect may prove to be vital in an unforeseen or novel disruption and a CCP must have the ability to act appropriately given the prevailing facts and circumstances, including determining when a stressed exit strategy should be used and what form that exit may take (e.g., appropriate recovery time, where applicable). A CCP must be able to consider the nuances of determining when a stressed exit would be appropriate (or not) and as such, a CCP should have the ability to build the necessary flexibility into its contracts and other documentation with respect to a potential exit strategy and should not be expected to granularly define a strategy given the numerous potential fact patterns of an event. Additionally, we note that the Consultation appears to granularly define expectations on the governance surrounding exit plans (as well as business continuity plans), which we believe should be left to the CCP, as that will allow a given CCP to assign clear roles and responsibilities regarding its plans that are appropriate for its individual structure, which inherently varies across CCPs. Further, it must also be recognized that an exit plan is different than a contingency plan which may allow the contractual arrangement to continue but seek an alternative means to provide the service.

Additionally, exit strategies for intragroup services, should be excluded here as the exiting of these services may have far reaching impacts beyond the service in question. This is especially true of intragroup agreements for information, communications, and technology systems which, upon exit, would require the business to find an external entity to provide technology services. Further, other intragroup services that require technology for delivery would be significantly disrupted.

XI. About CCP12

CCP12 is the global association for CCPs, representing 40 members who operate over 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@ccp12.org or through our website by visiting www.ccp12.org.

XII. CCP12 Members