Date: 30 September 2020

Giles Ward
International Organization of Securities Commission (IOSCO)
Calle Oquendo 12
28006 Madrid
Spain

Dear Sirs and Madams,

GFMA Consultation Response: IOSCO Principles on Outsourcing

Public Comment on Principles on Outsourcing

The Global Financial Markets Association ("GFMA[1]") welcomes the opportunity to comment on IOSCO's Principles on Outsourcing Consultation Report (CR01/2020) ("Consultation Report") published in May 2020. The Consultation Report proposes a set of fundamental precepts and seven principles covering issues such as the definition of outsourcing, the assessment of materiality and criticality, affiliates, sub-contracting and outsourcing on a cross-border basis ("Principles on Outsourcing" or "Principles").

We note that IOSCO has previously published Outsourcing Principles for Market Intermediaries in 2005 and Outsourcing Principles for Markets in 2009. However, this review expands the application of the proposed Principles on Outsourcing to trading venues, market intermediaries, market participants acting on a proprietary basis, credit rating agencies and financial market infrastructures.

Introduction to the GFMA

The GFMA represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows, benefiting broader global economic growth.

[1] The Global Financial Markets Association ("**GFMA**") brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, please visit http://www.gfma.org.

The Association for Financial Markets in Europe ("AFME[2]") in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association ("ASIFMA[3]") in Hong Kong and the Securities Industry and Financial Markets Association ("SIFMA[4]") in New York and Washington are, respectively, the European, Asian and North American members of the GFMA.

High-Level Response

The GFMA has several overarching comments that we believe are essential for IOSCO to address in connection with the proposed Principles on Outsourcing. In particular, we believe that:

- **there is a strong need for international harmonization in regulatory approaches**: A recurring theme across our responses to the questions posed by IOSCO is the risk of regulatory fragmentation across different jurisdictions. As a global standard organization, we believe it is important for IOSCO to strive for convergence in regulatory approaches (particularly, with existing regulatory frameworks which financial firms have already adopted, such as the Final Report on EBA Guidelines on outsourcing arrangements ("EBA Guidelines") published by the European Banking Authority ("EBA")). This is of paramount importance as our members firmly believe that regulatory fragmentation would lead to unintended consequences which are detrimental to the overall financial sector. In particular, we focus on three key categories of unintended consequences as follows:
    - **Impact on end-users**: Fragmentation creates undesirable impacts on end-users, including end-investors served by the financial system. These include higher fees (pricing reflecting higher cost of operating across fragmented regulatory requirements) and constraints on access to products and services;
    - **Impact on market development**: Fragmentation impedes the growth of domestic and cross-border financial markets by raising barriers to entry. In extreme scenarios, fragmentation can lead to market retraction and exit by participants as the complexity and costs of doing business become uneconomic; and

[2] The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. We represent 177 members – universal banks, investment banks, and other relevant institutions such as law firms and credit rating agencies – who have operations in 30 European countries

[3] ASIFMA is an independent, regional trade association with over 125 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

4 SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate on legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development.

- **Impact to financial sector and financial stability**: Fragmentation also increases the complexity of risk management across financial markets, heightening the overall risk to financial stability.

Accordingly, we believe that IOSCO should look to implement a set of revised Principles on Outsourcing in a manner which is generally consistent with other regulatory approaches;

- **there should be further clarity on the scope of the term "Outsourcing" and well-established definitions should be leveraged:** Whilst we support the inclusion of a section to define the scope of "Outsourcing" as a fundamental precept to the Principles on Outsourcing, we believe that the proposed definition should leverage existing, well-established definitions. In particular, we note the following areas of key concern:
  - the concept of "purchasing" in determining whether a transaction constitutes an "Outsourcing" transaction should be removed. Instead, we believe IOSCO should adopt a similar or consistent approach to those of the EBA (and proposed by the European Securities and Markets Authority ("ESMA") under its consultation on the draft guidelines on Outsourcing to Cloud Service Providers);
  - we believe that a "continuous basis" element should form part of the definition of an "Outsourcing" transaction. We refer to the EBA's definition of Outsourcing under the EBA Guidelines which requires an assessment to be made on whether an outsourced function is performed on a "recurrent or an ongoing basis"; and
  - furthermore, we believe it is inappropriate to define "Outsourcing" to include tasks which regulated entities "could in principle" undertake itself, but that it should be tied to a "realistic" possibility that the tasks could be carried out by the regulated entity;
- **the definition of "materiality" / "criticality" should be further clarified:** Although we welcome flexibility in deciding upon a list of factors influencing "criticality" and "materiality", IOSCO should consider the adoption of a single standard (be it, either "materiality" or "criticality") to reduce ambiguity. There is also a strong preference amongst our members for IOSCO to align the particular threshold with the concept of "critical or important function" under the EBA Guidelines;
- **the approach on data access and data localization should be further considered:** We are concerned that the language in Principle 6 provides that a regulator may be granted direct access to the systems and premises of regulated entities' service providers. In particular, we believe regulated entities should be aware of any regulatory requests (as is the case for regulatory access / dawn raids on the regulated entity's premises) and that regulated entities should have visibility of the nature of the regulatory request. Such an approach may potentially override the operation of (or otherwise result in the waiver of) legal professional privilege to the extent any such documents are protected. Principle 6 also expressly contemplates that jurisdictions and regulators may impose specific requirements concerning access to data which may include requiring records to be maintained in the regulator's jurisdiction (including, where relevant, in a locally stored back-up of the relevant data). Such reference creates significant potential for data localization requirements. This is of significant concern as data localization policies may restrict cross-border capital flows directly, such as ringfencing policies that impose capital requirements or activity

restrictions, or indirectly such as requirements on physical location of supporting infrastructure and activities. This reduces interconnectedness of the host country with the global system, and undermines the efficient deployment of capital, flow of liquidity and information, and overall financial stability; and

- **regulators should be responsible for measuring concentration risk at industry level and should closely consult financial firms in devising any regulatory measures to address concentration risk:** We believe the onus to measure concentration risk arising from a limited number of service providers servicing certain regulated markets should be performed (and managed) by the respective regulators. However, we caution against the introduction of regulatory measures to address concentration risk which could potentially impact the ability of a regulated entity to manage its oversight obligations, continuously enhance its resilience capabilities, adapt to emerging business models and technologies, and make commercial decisions. Financial firms are particularly concerned of regulatory measures which mandate use of multiple service providers (to the detriment of other commercial / operational considerations) in circumstances where regulated entities are able to manage the concentration risk which arises from use of the same service provider. Any regulatory approaches should be considered in close consultation with financial firms.

In addition, we wish to point out a high-level concern relating to the Principles on Outsourcing more generally. Due to the nature of IOSCO, financial firms recognize that it is up to each IOSCO member to adopt the Principles on Outsourcing within the various jurisdictions in which they operate and those in-country regulators may choose to adopt all, some or none of these Principles on Outsourcing (or may even choose to "gold-plate" certain areas). Financial firms are thus concerned that these Principles on Outsourcing – whilst welcome -may not be sufficient to forward regulatory convergence). We believe it is important for IOSCO to make a conscious effort to seek to harmonize the various approaches to regulating outsourcing transactions and as mentioned above, also align the principles with existing, well-established regulatory requirements and guidance such as those of the EBA.

* * * * *

In addition to the comments above, the GFMA is providing in the attached document specific responses to each of the questions put forward in the Consultation Report.

This response has been drafted with the support of Eversheds Sutherland, based on feedback from AFME, ASIFMA and SIFMA members.

Concluding Remarks

In general, the GFMA and its members support IOSCO's initiative to update the Principles on Outsourcing and to expand the application of the Principles to other areas of the financial services sector. However, we believe it is imperative for IOSCO to conduct its review of the Principles in close consultation with the industry and with regard to other regulatory approaches with an overarching strategy of minimizing regulatory fragmentation. As an international association constituted of

regulators from across various jurisdictions, we believe IOSCO is well placed to lead coordination efforts to seek to harmonize the approach to regulating outsourcing transactions.

We and our members stand ready to engage on this topic further with IOSCO (and members of IOSCO). We look forward to having the opportunity to provide further assistance as regulations governing outsourcing transactions continue to be refined.

Respectfully,

Allison Parent

Executive Director

Global Financial Markets Association

www.gfma.org

Questions for Public Consultation – GFMA Reponses

Chapter 3 – Fundamental Precepts

Question 1. Do you consider the scope of the application of the Principles to entities is clear? If not, why not?

- We request that IOSCO provide further clarification on the application of the Principles to regulated entities as set out on pages 5 and 6 of the Consultation Report. The Principles on Outsourcing are stated to apply to "trading venues, market intermediaries and market participants acting on a proprietary basis, credit rating agencies and financial market infrastructures." However, it is not at all clear whether the Principles only apply to regulated entities to the extent such entities are outsourcing activities related to those roles specifically, or whether the Principles apply to all activities undertaken by the regulated entities (regardless of the activity that is being outsourced) provided that one part of the regulated entities' business is within the scope of Committees 2, 3, 6 or 7.
- In addition, it is noted that the Consultation Report refers to the terms "market intermediaries and market participants" being applied as appropriate in the context of "jurisdictional differences in regulatory scope". We request further clarification on how these terms are intended to interoperate with local regulatory requirements pertaining to outsourcing, particularly where the central bank and securities regulations in a given jurisdiction are likely to differ in their application and approach.
- Further, we believe the scope of the application of the Principles can be further clarified as set out in our response to Question 2 below.

Question 2. Do you consider the concepts used to explain the application of the Principles on Outsourcing to be clear and adequate? If not, why not?

- We support the inclusion of a section to define the scope of "Outsourcing" as a fundamental precept to the Principles on Outsourcing. However, we believe that the proposed definition and accompanying explanation should leverage existing, well-established definitions, remove the concept of "purchasing", incorporate a "continuous basis" element and take into account whether a service can realistically be performed by the regulated entity. The definition should also exclude activities which are legally required to be provided by an external service provider.

Concept of "purchasing"

- Under paragraph 1 of page 7 of the Consultation Report, IOSCO distinguishes the concept of "Outsourcing" from the concept of "purchasing contracts", which are not to be taken to be "Outsourcing" transactions. The term "purchasing" is defined within the Consultation Report as "the acquisition from a vendor of services, goods or facilities without the transfer of, access to, or responsibility for the handling of the purchasing entity's non-public proprietary or client information."

- However, we believe that the use of the concept of "purchasing," as it is currently defined, is potentially problematic. By way of example, financial firms often rely on third parties for managed services of computer equipment or infrastructure that is owned by the regulated entity. However, the third-party personnel engaged in the provision of the managed services do not necessarily have logical access to the non-public proprietary or client information stored on the equipment. Arguably this is a service that the regulated entity would otherwise undertake itself, yet under these Principles, it is unclear whether such a procurement would constitute an "Outsourcing" or a "purchasing contract".
- Conversely, the outsourcing of receptionist services will likely involve the provision of client confidential information or proprietary confidential information to the service provider (e.g. the regulated entity's client details). Under the current definition, such services would fall within the scope of "Outsourcing". However, these type of services are not generally considered to be outsourcing, as expressly stated under paragraph 28(g) of the European Banking Authority's ("EBA") Final Report on EBA Guidelines on outsourcing arrangements ("EBA Guidelines").[5]
- Therefore, the reliance on the concept of "purchasing" leads to the critical factor (in determining whether a transaction is an "Outsourcing" transaction or not) being the question around non-public proprietary or client information. This emphasis may lead to inconsistencies with other regulations if applied.
- We believe that IOSCO should remove the concept of "purchasing" in determining whether a transaction constitutes an "outsourcing" transaction. We refer IOSCO to the approach adopted by the EBA (and proposed by the European Securities and Markets Authority ("ESMA") under its consultation on the draft guidelines on Outsourcing to Cloud Service Providers) as summarized below. These guidelines were previously widely consulted on and are accepted by the industry as setting the benchmark for best practice.
    - Under the EBA Guidelines, institutions and payment institutions are required to assess whether a function is outsourced to a service provider by considering whether the function:
        - is performed on a recurrent or an ongoing basis; and
        - would normally fall within the scope of functions that would or could realistically be performed by institutions or payment institutions (even if the institution or payment institution has not performed the function in the past itself).
    - The EBA further sets out a list of functions that should not generally be considered as outsourcing as per paragraph 28 (such as a function that is legally required to be performed by a service provider, e.g. a statutory audit), which is an approach we would encourage IOSCO to consider adopting.

[5] European Banking Authority. Final Report on EBA Guidelines on outsourcing arrangements (25 February 2019). Retrieved from: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

- Similarly, under ESMA's consultation on Outsourcing to Cloud Service Providers[6], the proposed definition of a "cloud outsourcing arrangement" is assessed by reference to whether the arrangement involves the delegation of a function that would otherwise have been undertaken by the firm itself.

- In light of the significant consultation work that has been undertaken (and is being undertaken) by the above regulators, we believe that IOSCO should adopt a similar or consistent approach by removing the concept of "purchasing contracts" in the definition of "Outsourcing". This will assist in driving regulatory convergence in this area, which is of paramount importance to many financial firms that operate globally across a number of jurisdictions.
- If IOSCO does retain the concept of "purchasing", we believe that it would be helpful for IOSCO to further provide additional guidance and (if possible) supplementary illustrative scenarios and parameters to assist regulated entities in further distinguishing between "Outsourcing" and "purchasing" transactions.

<u>"Continuous basis" element</u>

- Furthermore, the definition of "Outsourcing" under the Consultation Report lacks a "continuous basis" element. We believe that this element should form part of the definition of an "Outsourcing" transaction under the Principles on Outsourcing.
- We refer to the EBA's definition of Outsourcing under the EBA Guidelines which requires an assessment to be made on whether an outsourced function is performed on a "recurrent or an ongoing basis".
- We also refer to the definition of "outsourcing arrangement" adopted by the Monetary Authority of Singapore ("MAS"), which categorizes an arrangement to only be an "outsourcing arrangement" if an institution is dependent on the service on an ongoing basis.[7]
- As noted above, we consider it critical for IOSCO to adopt a consistent approach to drive regulatory convergence in this area.

<u>Possibility of service being carried out by regulated entity</u>

- We also believe that it is not appropriate to define "Outsourcing" to include tasks which regulated entities "could in principle" undertake itself, but that it should be tied to a "realistic" possibility that the tasks could be carried out by the regulated entity. The scope adopted by IOSCO extends the definition of "Outsourcing" beyond the definitions set out under the current regulations.

---

6 European Securities and Markets Authority. Consultation Paper – Draft Guidelines on Outsourcing to Cloud Service Providers (3 June 2020). Retrieved from: https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf

7 Monetary Authority of Singapore. Guidelines on Outsourcing (which effect from 8 October 2018). Retrieved from: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf

- It is observed that regulated entities globally are undertaking significant technology and digitalization projects, with investment in key technology solutions and accompanying capability likely to increase over time. Accordingly, the tasks that a regulated entity "could in principle" undertake will likely create further ambiguity in performing this assessment.
- We refer IOSCO to the EBA Guidelines which categorize whether a function has been outsourced by assessing whether the function would "normally" fall within the scope of functions that would or could "realistically" be performed by institutions or payment institutions.

Other concerns

- It is unclear how this Consultation Report interacts with the Principles for Financial Market Infrastructure published by the Bank for International Settlements (including the existing function of Annex F for Critical Service Providers).[8] We believe that IOSCO should provide commentary on how different guidance from various regulators should interact. It should also be considered that "Outsourcing" as used in the context of this Consultation Report should not cover payment schemes (FMIs) which split schemes from the switch and technical infrastructure.

Question 3. Do you have any comments on the benefits, risks, and challenges of the use of outsourcing? Are there any additional factors which should be considered or described in the document?

- As an overarching comment, we note that the manner in which this question was phrased focuses only on Sections D and E (and not on Section C). Accordingly, our comments in respect of Section C (if any) are set out in our response to Question 13.
- We believe that the section entitled "Operational resilience" in Section E should more clearly articulate the outsourcing risks and challenges of regulated entities and regulators. This would assist in contextualizing the rationale for updating the Principles on Outsourcing. In its current form, the section addresses general operational resilience risk without "contextualizing its importance specifically to Outsourcing".
- Additionally, Sections D and E - and the Consultation Report more generally – do not consider how the Principles should be applied to financial firms of various sizes in a proportionate manner. We believe that IOSCO should provide guidance on the appropriate frameworks to apply which are proportionate to the size of the financial firms. We refer to the Consultation Paper on Outsourcing and third party risk management by the Prudential Regulatory Authority ("PRA"), which proposes that firms meet the expectations set out under its draft Supervisory Statement "in a manner appropriate to their size and internal

[8] Bank for International Settlements. Principles for financial market infrastructures (16 April 2012). Retrieved from: https://www.bis.org/publ/cpss101a.pdf

organization and the nature, scope and complexity of their activities, in line with the principle of proportionality".[9]

Question 4. Does the description of materiality and criticality clearly and adequately address the proportional application of these principles? If not, why not?

- We welcome flexibility in deciding upon a list of factors influencing "criticality" and "materiality". However, to reduce ambiguity, IOSCO and global standard organizations more generally should consider the adoption of a single standard (be it, either "materiality" or "criticality") provided that such standard retains flexibility for regulated entities to determine what they deem to be "critical" or "material" in the context of the particular outsourced services.
- There is a strong preference from members for IOSCO to align the particular threshold (be it "materiality" or "criticality") with the position adopted by the EBA under the EBA Guidelines. If such a position is adopted, IOSCO should make clear that the "materiality" or "criticality" threshold is intended to align with the concept of "critical or important function" under the EBA Guidelines. Our members wish to avoid a situation similar to the concurrent PRA consultation under which the PRA appears to define "material outsourcing" in its consultation paper more broadly than the term "critical or important function" as adopted by the EBA without providing additional specific guidance on how it intends "material outsourcing" to be interpreted.
- It is noted that the EBA takes a clearer approach in defining whether an outsourcing activity is "critical or important" by deeming certain functions to be "critical or important" if they result in certain consequences (e.g. where a defect or failure in the performance of the outsourced function would materially impair a regulated entity's continuing compliance with the conditions of its authorization). The EBA then lists other factors which regulated entities must take into account in assessing whether certain functions are "critical or important". In contrast, IOSCO has only provided factors which regulated entities will need to take into account in assessing "materiality" or "criticality" (without providing clarity on whether certain functions would be deemed by IOSCO as such). We believe IOSCO should consider adopting a similar approach to the EBA to clarify the "material" and/or "critical" threshold.
- Further, based on the drafting of the Consultation Report, it would appear that an activity that meets any one of the factors to be considered in assessing whether an activity is "material" or "critical" would be sufficient to elevate that activity to be a "material" or "critical" outsourcing. If that interpretation is correct, this definition would capture a broad range of activities and appear likely to result in a much lower threshold of "materiality" or "criticality" than that of the EBA's "critical or important function" definition. This is likely to lead to uncertainty on how regulated entities are to practically comply with IOSCO's requirements given the Consultation Report lacks clear guidance on the steps regulated

[9] Prudential Regulation Authority. Consultation Paper – Outsourcing and third party risk management (December 2019). Retrieved from: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf?la=en&hash=393834B1FDE05A8571522FD72A6A8D997079714C

entities are expected to take. Regulated entities are only required to apply the Principles according to the degree of "materiality" or "criticality" of the outsourced tasks. Such a difference in regulatory approaches is also likely to lead to additional complexity and costs in the procurement of outsourcing services. As noted above, it is of paramount importance to financial firms for there to be convergence in outsourcing regulations.

- Additionally, as a general comment, we feel that the use of examples focusing on credit rating agencies ("CRA") to provide context to the guidance set out in the Consultation Report (and in the context of Section F, the difference between the terms "material" and "critical") is of limited assistance to many financial firms given the atypical nature of CRAs.
- We also note that it is not appropriate for the last three bullets of Section F (set out on pages 11 and 12 of the Consultation Report) to be included as part of a "materiality" or "criticality" assessment. For clarity, these bullets refer to:
    - the degree of difficulty and the time required to select an alternative service provider or to bring the task in-house;
    - aggregated exposure to a service provider in cases where the regulated entity outsources various tasks to the same service provider; and
    - aggregated risk exposure due to industry-wide concentration of outsourced materials or critical services to the same provider.

  We believe that these factors are more appropriately included as part of a regulated entity's ongoing "risk management" exercise (rather than a "materiality" or "criticality" assessment). Please also refer to our response to Question 10 below in respect of the concentration risk.
- Additionally, in respect of the fifth last bullet of Section F (assessing the involvement of critical information), financial firms acknowledge it could be taken into account as part of a "materiality" or "criticality" assessment. However, the factor should not, in and of itself, be a determining factor. It must be considered in light of all factors, noting that almost all information handled by financial firms is considered "client-confidential".
- As a general observation, we understand that IOSCO intends for regulated entities to apply the Principles on Outsourcing on a risk-based approach. That is, the Principles on Outsourcing are to apply in a manner that is proportionate to the "materiality and criticality" of the outsourced transaction. We believe that IOSCO should make this expectation clearer within the Principles on Outsourcing and IOSCO should provide further guidance on how this concept of proportionality should be applied by regulated entities. We refer IOSCO to the EBA Guidelines which identify specific steps that institutions and payment institutions are expected to take in respect of "critical or important functions".

Chapter 4 – Outsourcing Principles

Question 5. Do you consider the Principle and implementation measures for due diligence are adequate and appropriate? If not, why not?

- Whilst we generally support the due diligence implementation measures set out in this Principle 1, we note that under Section I of Chapter 3, the Consultation Report requires regulated entities to consider the ability of the sub-contractor to continuously perform the

services, as part of its due diligence process under Principle 1. Principle 1 requires regulated entities to, amongst other steps, implement monitoring measures in respect of its service provider's ability and capacity to undertake the outsourced tasks.

- We believe that it is not appropriate for due diligence conducted in respect of a sub-contractor to be undertaken to the same level of detail and scrutiny as compared with due diligence conducted of a service provider which is directly contracted by a regulated entity. In many instances, regulated entities would not be granted the same level of direct access to the sub-contractors for the purpose of undertaking the due diligence referred to in Principle 1. Furthermore, regulated entities generally have the contractual benefit of its service providers being liable for the services provided by its sub-contractors.
- In light of the above, IOSCO should expressly recognize under the Principles on Outsourcing that due diligence conducted in respect of a sub-contractor should be of a standard that is more proportionate to the risk involved.
- Further, financial firms require IOSCO to clarify that the term "sub-contractors" refers only to those sub-contractors of outsourced service providers (and is not intended to refer to the contractors of those sub-contractors). Financial firms understand that IOSCO is not requiring regulated entities to be responsible for all parties along the supply chain. Please also refer to our further response to Question 13 below in which we submit that regulated entities can manage the sub-contracting arrangements by adopting an approach similar to the EBA Guidelines by specifying whether the sub-contracting of "critical or important functions" (or activities which are considered to be "material" or "critical") is permitted.
- Additionally, we consider the documentation requirements under Principle 1 should not merely create a "tick box" exercise. It would be particularly useful if IOSCO can provide further guidance on the scope and level of detail to be covered under such documentation (particularly if IOSCO's view is that the documentation required could vary depending on the "materiality" and/or "criticality" of the particular activity).
- Finally, we believe that the relationship between accountability for selection of the outsourced service provider and accountability for actual performance of the outsourced service requires greater clarity. In particular, the Consultation Report provides that a regulated entity "should always maintain a minimum operational and managerial capability". This requirement appears to apply regardless of the extensiveness of the due diligence undertaken and the nature of the outsourced activity. We believe whether a regulated entity is required to maintain operational capability should be dependent on the "materiality" or "criticality" of the outsourced activity and should also take into account the due diligence process.

Question 6. Do you consider the Principle and implementation measures for establishing the contract with a service provider are adequate and appropriate? If not, why not?

- Principle 2 requires regulated entities to consider the inclusion of provisions into legally binding written contracts with service providers that provide for access of records and information, premises, IT systems and personnel concerning outsourced tasks to regulators. For the reasons detailed in our response to Question 11 below, we have concerns in relation

to regulators having the direct right to access such information from regulated entities' service providers.

- Additionally, we believe that the Consultation Report must expressly recognize that the requirements set out in Principle 2 are not suitable for intra-group outsourcing or where the activity is outsourced to a separate branch of the same legal entity (as a contract cannot be formed between the same entity, e.g. in a branch-to-branch contracting scenario). IOSCO should provide guidance on how Principle 2 is expected to be met in the context of intra-group / inter-branch outsourcing arrangements. In the experience of our members, certain local regulators have been satisfied by a written letter between the intra-group entities / branches outlining the key details of the outsourced activity.
- As a final comment, it is noted that the second to last bullet point (on page 19) appears to be a duplicate of the third bullet point (on page 18).

Question 7. Do you consider the Principle and implementation measures for information security, business continuity and disaster recovery are adequate and appropriate? If not, why not?

- We have a number of concerns regarding the implementation measures for information security, business continuity and disaster recovery set out in Principle 3, detailed as follows.
- However, in general, we note the need for these requirements to be implemented in a proportionate way. Some outsourcing relationships may not warrant the level of IT security controls indicated under Principle 3.

Cyber frameworks

- Under the last bullet point of the section entitled "Implementation", IOSCO seeks to leverage existing cyber frameworks to address information security, business continuity and disaster recovery risks faced by regulated entities. We believe that SOC 2 audit controls should be included in that list of cyber frameworks. Additionally, we also recommend that the Financial Services Sector Cybersecurity Profile ("Profile") should constitute one of the frameworks that regulated entities could leverage.[10] The Profile is based off the NIST Cybersecurity Framework, CPMI-IOSCO's "Guidance on cyber resilience for financial market structures", ISO/IEC 27001/2 and tailors the controls specifically to the financial services sector. As IOSCO pointed out in its June 2019 Cyber Task Force Report, the Profile "is a customization of the NIST Cybersecurity Framework that financial institutions can use for internal and external cyber risk management assessment and as evidence for compliance, encompassing relations between Cyber frameworks, including Core Standards (being the NIST Cybersecurity Framework, ISO, and the CPMI-IOSCO Guidance)."[11]

[10] Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. The Financial Services Sector Cybersecurity Profile (Profile), v1.0 (last updated October 2018). Retrieved from: https://cyberriskinstitute.org/the-profile/

[11] The Board of the International Organization of Securities Commissions. Cyber Task Force – Final Report (June 2019). Retrieved from: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf

Open-source resources

- Under the third bullet point of page 21 of the Consultation Report, IOSCO appears to have conflated the concepts of "subcontracting" and use of "open-source resources". We believe that IOSCO should provide a definition of "open-source resources" and further guidance on its expectations to the extent open-source resources are used by regulated entities' service providers, and specifically provide clarity on its reference to "open-source resources". Is this intended to refer to open-source software?
- We do not believe it is appropriate to apply the same requirements applicable to the use of subcontractors to the use of "open-source resources" by service providers. Open-source resources are widely used and provide an important security control as they are exposed to security scrutiny by the entire developer community. While we would expect that appropriate due diligence is undertaken in relation to these resources, we would not expect the same requirements applicable to sub-contracting to be imposed on open-source resources.

Pooled audits, third-party certifications and audit reports

- We also believe that pooled audits (as well as third-party certifications and external/internal audit reports made available by the service provider) should be expressly specified as a way in which regulated entities could manage the security, business continuity and disaster recovery risks which Principle 3 seeks to address. It is unclear to us why "pooled audits" are expressly mentioned in respect of Principle 6 only. Although the last bullet point of the section entitled "Implementation" under Principle 6 states that regulated entities should look to and implement existing cyber frameworks to address the risk, it should be made clear that regulated entities can rely on third-party certifications and external/internal audit reports provided by the service provider.
- We refer to the EBA Guidelines which permit institutions and payment institutions to use pooled audits, third-party certifications and external/internal audit reports generally as part of institutions and payment institutions' monitoring of outsourced functions (although the final responsibility in relation to the outsourcing arrangements remain with the institutions and payment institutions). This approach also aligns with proposals made by ESMA under its consultation and PRA in its consultation paper.

Portability

- The final paragraph on page 21 of the Consultation Report implies that the only acceptable mechanism for ensuring business continuity is the transfer of the outsourced service and tasks. While these may be appropriate options to consider in the event of a breakdown in the vendor relationship, we caution that they should not be considered to be appropriate contingency plans in the event of a service provider outage. Any attempt to migrate services or data during an IT incident could result in further operational risks. In the event that a service provider works with multiple regulated entities, regulatory requirements that result

in the mass migration of services away from that service provider could destabilize the market.

- Existing regulations generally already require regulated entities to ensure the continued provision of the outsourced services and continued access to data. Our view is that the transfer of service is feasible in the event of a medium to long term migration away from a service provider in a planned manner but is not appropriate to address business continuity risk in the event of an IT incident.

Other

- In the third paragraph under Principle 3, IOSCO states that the entity must account for "whether additional issues" are raised as a result of cross-border outsourcing. We do not believe "cross-border" is a relevant determinant of risk. Rather, the entity should assess the risks arising from the legal and/or political circumstances of the location from where the outsourced service is performed. We believe this would result in the same due diligence being undertaken by regulated entities whether or not the relevant outsourcing involves cross-border outsourcing.
- In respect of the first bullet point on page 21 of the Consultation Report, regulated entities are required to ensure that there are provisions in the contract with service providers specifying the rights of each party to change or require changes to security procedures and requirements and of the circumstances under which such changes might occur. This requirement is very broad and generic in nature.
- Under the second bullet point on page 21 of the Consultation Report, there is a reference that service providers may be required to maintain back-ups in the jurisdiction of the regulated entity. For the reasons set out in our response to Question 11 under "Data Localization", this requirement could prove problematic if it were adopted by multiple regulators. It may frustrate firms' ability to execute their own cloud and associated resiliency strategies and may impede cloud uptake due to the indirect "data localization" impact. Any decision to duplicate data should be made by regulated entities on a case-by-case basis and with consideration given to the regulated entities' resilience strategy.
- We also refer to the fourth bullet point on page 21 of the Consultation Report, under which regulated entities are required to consider incorporating in the relevant outsourcing contract, where appropriate, the requirement for the service provider to test its processes, systems and back-up facilities critical to their business on a periodic basis. We believe that, for certain outsourcing transactions where there is limited need to ensure the constant availability of data, it would be sufficient for the regulated entity to guarantee the return of data when needed (and /or at the end of the contract).
- Finally, under bullet point 5 on page 21 of the Consultation Report, it should be clarified that the disclosure of security breaches by the service provider should only be to the regulated entity (and not to the wider market or the regulated entity's regulators).

Question 8. What measures for business continuity would be effective in situations where all, or a significant portion, of both the outsourcers' and third-party providers' work force is working

remotely? In particular what steps should be taken with respect to Cyber Security and Operational Resilience?

- While COVID-19 is an unprecedented event in many respects, the plans, processes, and tools financial firms already had in place to protect against a disruptive cyber event are generally working as planned. Given that in the industry the vast majority of employees worked from home ("WFH"), financial firms' network and IT infrastructure proved they can support mission-critical and essential workers, as well as administrative users, for long periods of time. While the WFH access methods used uncovered some improvements firms could make to the resiliency of the infrastructure, all have contributed to make firms into more stable organizations. Financial firms are also taking the following steps, which are repeatable for future events:
    - increasing infrastructure capacity for remote workforce and enhanced alerting capabilities to detect potentially malicious access attempts;
    - enhancing specific controls to safeguard remote access sessions, such as detections to identify brute-force login attempts and preventative controls to block users from copying firm information onto personal devices;
    - reinforcing baseline security practices for the remote workforce including targeted messaging to users to remind them of policies or special entitlements;
    - maintaining transparent and proactive communications with vendors to meet both risk management and regulatory requirements and ensure business continuity processes (BCP) with critical vendors are implemented in the event of an incident;
    - reviewing and confirming Distributed Denial of Service (DDOS) mitigation plans, particularly for the remote login infrastructure;
    - updating long-term enterprise security strategies and policies for firms and third parties to ensure appropriate coverage in the event of a second or third wave or another contingency event similar to COVID-19;
    - monitoring for additional Data Loss Prevention (DLP) and security exposures;
    - performing real-time, ongoing, organization-wide remote workforce testing;
    - strengthening security controls for existing digital services (e.g. VPN infrastructure); and
    - strengthening awareness initiatives regarding cyber risks related to the pandemic.
- Further, we note that the precise scope of the question is unclear. On one hand, it appears that IOSCO is seeking feedback in relation to the impact WFH arrangements are having on business continuity measures (i.e. from a service level / degradation perspective), however, the second component of the questions suggests that the primary concern is potential cyber security and operational resilience risk which may arise during these remote working arrangements. The above response sets out measures taken to address both business continuity and/or cyber security and operational resilience risks.
- Finally, we note that there are a number of current open consultations in relation to both cybersecurity and operational resilience (e.g. BCBS consultation on principles for operational resilience, PRA and FCA consultations on operational resilience) and we encourage IOSCO to

be part of such discussions and lead coordination efforts to minimize the risk of fragmentation in regulatory approaches.

Question 9. Do you consider the Principle and implementation measures for the management of confidentiality issues are adequate and appropriate? If not, why not?

- We generally support the inclusion of Principle 4 which requires regulated entities remain in control of how their data is used by service providers.
- However, under Principle 4, IOSCO considers that in respect of Credit Rating Agencies ("**CRAs**"), "confidential information should be understood to not only include information related to the CRA itself, but to any issuer, obligor, subscriber or investor-related information and/or software." We disagree with the inclusion of "software" under this Principle. We request IOSCO to clarify why "software" is expressly referenced in that paragraph given that the remaining sections of this Principle do not otherwise address or refer to the disclosure of "software".
- Further, we believe it should be clarified that the implementation section of Principle 4 should be read consistently with, and is not intended to conflict with, local data protection laws, for example, GDPR.
- Finally, in line with our response to Question 4, we reiterate that the Consultation Report's focus on the CRAs is not appropriate given the atypical nature of their operations (and should not be the primary driver of IOSCO as the scope of the Consultation Report (and its application) extends beyond CRAs). The Consultation Report should provide guidance applicable to all regulated entities.

Question 10. Do you consider the Principle and implementation measures for the management of concentration risk in outsourcing arrangements are adequate and appropriate? If not, why not?

- We recognize that it is the responsibility of each regulated entity to address concentration risk arising from the reliance of certain service providers by that regulated entity. Regulated entities generally already perform their own concentration risk assessments as part of their ongoing risk management process for outsourcing arrangements. Based on these assessments, the regulated entity may, if necessary under a risk-based approach, take action to address such concentration risks (e.g. increasing the control and security expectation on the service provider or using two or more regional or global providers for a given service).
- However, the onus to measure concentration risk arising from a limited number of service providers servicing certain regulated markets should be performed (and managed) by the respective regulators. It is noted that regulators should closely consult with financial firms in introducing any regulatory measures to address concentration risks (as detailed in the fourth dot-point of this response below).
- We consider it is critical to make this distinction as, in practice, it would be extremely difficult for regulated entities to assess the concentration of particular industries due to a

lack of publicly available information regarding the service providers engaged by other regulated entities.

- We also caution the introduction of any regulatory measures to address concentration risk which could potentially impact the ability of a regulated entity to manage its oversight obligations, continuously enhance its resilience capabilities, adapt to emerging business models and technologies, and make commercial decisions. In particular, financial firms are particularly concerned of regulatory measures which mandate use of multiple service providers (to the detriment of other commercial / operational considerations) in circumstances where regulated entities are able to manage the concentration risk which arises from use of the same service provider.
- In regard to the final bullet point on page 25, we refer to our previous comments on the appropriateness of relying on the portability of an outsourced service in the event of an IT incident. While, in some limited instances, it may be technically feasible to design a go-live back-up, in light of the market concentration risk, such a substitution would create significant operational risk owing to the potential for large-scale migration of services from one provider to another (thereby potentially stressing the alternative provider's capacity). This is even more likely in instances where data localization rules or other regulations limit the ability of the service provider to rely on their entire global infrastructure.
- Further, a number of members had indicated a willingness to disclose to regulators the particular entities to which they outsource for the purpose of assisting the regulators in assessing concentration risk (and that, in fact, some are required to do this under existing local requirements). However, to the extent regulated entities are required to disclose such information, we believe IOSCO has an important role to play in harmonizing the disclosure requirements so that regulated entities do not have to provide different reports to regulatory authorities in different jurisdictions. We are certainly aware that there is widespread interest amongst regulators in respect of this topic and a key concern of members is that regulators will adopt individual regulatory policies to address what is often a cross-regional risk. This will result in a fragmented financial market with correspondingly greater operational risks for regulated entities.
- In the context of concentration risk pursuant to Principle 5, we believe that IOSCO should expressly carve-out affiliate relationships (whether it is an intra-group or inter-branch outsourcing). The recommendations in this context are not suitable for scenarios where the regulated entity can exercise control over its affiliated outsourcing provider.

Question 11. Do you consider the Principle and implementation measures for ensuring access arrangements are adequate and appropriate? If not, why not?

- We have two specific key concerns in respect of Principles 6 as follows: (i) direct access to the relevant systems and premises of the service provider; and (ii) the "data localization" element. Other concerns regarding the language of Principle 6 are also detailed below.

<u>Direct access to the relevant systems and premises of the service provider</u>

- We are concerned that the language in Principle 6 states that a regulator's access of the systems and premises of regulated entities' service providers may be "direct or indirect (depending on regulatory requirements)". In particular, we have significant concerns regarding the ability of the regulator being granted direct access as:
    - we consider that a regulated entity should be aware of any regulatory requests (as is the case for regulatory access / dawn raids on the regulated entity's premises);
    - we consider a consent mechanism to be necessary to ensure the regulated entity has visibility of the nature of the regulatory request;
    - it may potentially override the operation of (or otherwise result in the waiver of) legal professional privilege to the extent any such documents are protected; and
    - a recent example has shown that service providers are generally very concerned about sharing records with the regulator without their clients' knowledge. It is noted that regulators have no jurisdiction over non-regulated service providers.[12]
- In the context of access to premises, the Consultation Report should recognize that for a service provider servicing a significant number of clients, it may not be feasible to offer access to all premises for inspection. In particular, major cloud service providers often cite the following reasons for rejecting access to their premises:
    - such access may create security risks;
    - such access may compromise client confidentiality; or
    - such access may simply not be achievable as a practical matter of scale.
- Further, in circumstances where the service provider is also a regulated entity itself, ensuring access to the service provider's systems could prove problematic as the service provider is also required to maintain confidentiality and integrity of its client data. Requests to accessing such service provider's systems may need to be dealt with on a case-by-case basis having regard to the nature of the service being provided and the scope of access required.

<u>"Data localization" element</u>

- Principle 6 expressly contemplates that jurisdictions and regulators may impose specific requirements concerning access to data which may include requiring records to be maintained in the regulator's jurisdiction (including, where relevant, in a locally stored back-up of the relevant data).
- Our principal concern is that such reference creates significant potential for data localization requirements. Localization policies may restrict cross-border capital flows directly, such as ringfencing policies that impose capital requirements or activity restrictions, or indirectly such as requirements on physical location of supporting infrastructure and activities. This reduces interconnectedness of the host country with the global system, and undermines the efficient deployment of capital, flow of liquidity and information, and overall financial stability.

[12] Hong Kong Securities and Futures Commission. Circular to Licensed Corporations - Use of external electronic data storage (31 October 2019). Retrieved from: https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/openFile?refNo=19EC59

- It is understood that the intention of regulators in prescribing data regulations is to protect data privacy, enhance data security, and promote the appropriate use of technology and big data. However, regulatory-driven fragmentation across jurisdictions results in increased operational risk, hinders the development of technology in financial services, and affects the provision of service to end-users. In particular, the following impacts are highlighted for IOSCO's consideration:
    - **Increased operational risk:** By requiring the duplication of data, processes and systems, data localization rules increase the complexity of the regulated entities' IT estates and thereby increasing their operational risk. Further, multiple data storage requirements for duplicated data increase the attack surface that regulated entities must defend against, resulting in increased cybersecurity risk. Accordingly, such rules often increase data privacy risk in a manner which is in direct contradiction with the policy objectives the rules were intended to achieve.
    - **Impact on end-users:** Per the International Institute of Finance ("IIF"),[13] data localization limits a bank's ability to leverage group solutions and rich data insights combining different sources of data to service the client. Under data localization constraints, an asset manager, for example, may be unable to aggregate and construct effective global portfolios for their client which limits the end users' investment and risk management capabilities.
    - **Impact on market development**: Allowing free flow of data is a catalyst for product development and effective risk management, especially given natural fragmentation in Asia Pacific capital markets. Research conducted by The European Center for International Political Economy ("ECIPE") indicated that economy-wide data localization laws could potentially drain between 0.7 per cent and 1.7 per cent from national GDP, and negatively impact market development and undermine economic growth.[14] While larger sized firms are often better equipped with capabilities and resources to comply with data localization requirements, small to medium sized enterprises or start-ups might not share the same privilege, and this would present barriers for some small players to participate in the market and form a vibrant ecosystem.
    - **Impact to financial sector and overall financial stability**: Barriers to cross-border information flow and systems and limitations on data sharing inhibit firms' ability to aggregate data and have a full oversight to provide better serve clients and manage risks. For example, data silo imposes challenges on financial crime supervision and successful monitoring of the cyber threat landscape.

[13] Institute of International Finance. Data flows across borders: overcoming data localization restrictions. (March 2019). Retrieved from: https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf

[14] European Center for International Political Economy (ECIPE). The Costs of Data Localization: A Friendly Fire on Economic Recovery (May 2014). Retrieved from: https://ecipe.org/publications/dataloc/

- Instead, we encourage that IOSCO supports cross border data flow in a manner outlined under the United States-Mexico-Canada Agreement (USMCA)[15] and the United States-Japan Free Trade Agreement (FTA), and further proposed in the United States-Singapore Joint Statement on Financial Services Data Connectivity, announced on 6 February 2020, and the Singapore-Australia Digital Economy Agreement (DEA)[16], announced in March 2020. We strongly support the approach adopted under the trade agreements and the Joint Statement, which facilitates the transfer of data by financial services firms across borders and opposes data localization requirements, subject to financial regulators having access to data needed for regulatory and supervisory purposes.
- The storage or backup of data in a local jurisdiction should be a decision that a regulated entity is able to initiate on its own accord, on a case by case basis. We do not agree that this should be enforced by regulators through the imposition of specific requirements to mandate the retention of records in the regulator's jurisdiction.

Other concerns

- We also have concerns in relation to the requirement that access to data should be in a form acceptable to the regulator (which includes both the format in which information is made available and the language in which the material is provided). We query how this element of Principle 6 is to be applied if data becomes less accessible due to encryption in line with good cybersecurity and data management practices (and regulatory requirements that might require encryption). We request IOSCO provides further clarity in respect of its expectation.
- Under the second last bullet point on page 28, regulated entities are required to ensure that they have appropriate plans for continued access by the regulator to books, records and appropriate personnel and systems in the event of the termination of a contract. We believe that IOSCO should expressly recognize that such a requirement will be time-bound and that the requirement is subject to record retention policies, requirements under privacy laws and other legal considerations.
- Principle 6 also stipulates that regulated entities may require contractual provisions which prohibit the service provider from deleting, discarding, or otherwise making unavailable, its records even in the event of non-payment of fees and charges by the regulated entity. This

---

[15] United States-Mexico-Canada Agreement (USMCA). Retrieved from: https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17-Financial-Services.pdf. We refer to Chapter 17 Financial Services, specifically: *Article 17.18: Location of Computing Facilities 1. The Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access. 2. No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory. 3. Each Party shall, to the extent practicable, provide a covered person with a reasonable opportunity to remediate a lack of access to information as described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of another jurisdiction.*

[16] Singapore-Australia Digital Economy Agreement (DEA). Retrieved from: https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement

reference is of particular concern because, in the experience of our members, third party service providers are unlikely to agree to the retention of records in the event of non-payment.

Question 12. Do you consider the Principle and implementation measures for the termination of outsourcing arrangements are adequate and appropriate? If not, why not?

- Whilst we consider the Principle and implementation measures proposed to be generally appropriate, we request that IOSCO provide further details on its expectations in respect of a termination under stressed and non-stressed scenarios (particularly in the context of exit planning and management – see comments above).

Question 13. Do you have any other comments on the Principles and implementation measures? Do you have any suggestions for other areas or risks IOSCO should address?

- In respect of Section G (Affiliates), the Consultation Report requires the Principles on Outsourcing to be applied to affiliate entities "where relevant" and notes that it "may also be appropriate to assess and apply them with some modification". This position is set out at quite a high-level and provides limited guidance to financial firms. We are concerned that this statement, without further guidance, will lead to different positions being adopted in various jurisdictions (rather than the harmonization of outsourcing requirements). We believe that IOSCO should provide further guidance and illustrative examples (where appropriate) on how it considers the Principles on Outsourcing should be applied in respect of intra-group and inter-branch transactions. In particular, we believe it is appropriate for a risk-based approach to be applied based on the context of the particular intra-group and inter-branch transactions. We also refer to our responses to Questions 6 and 11 above.
- In respect of Section I (Sub-contracting of outsourced tasks), the Consultation Report currently provides that sub-contracting is not permissible by a service provider without the relevant regulated entity's approval. We believe that IOSCO should adopt the approach set out within the EBA Guidelines under which sub-contracting of outsourced functions are generally permitted. To the extent that an outsourced function involves "critical or important functions" (as defined in the EBA Guidelines), the outsourcing agreement must specify whether the sub-contracting of such function by the service provider is permitted.
- Further, Section I (Sub-contracting of outsourced tasks) notes that a regulated entity should ensure it can continue to promptly access data maintained by the sub-contractors of the outsourcing service provider. We believe additional guidance is required to clarify whether IOSCO expects regulators and/or the regulated entity to have the right to directly access data held by the sub-contractor (or whether the ability to access the data hosted or stored by sub-contractors through the outsourcing service provider would be adequate to meet the requirement set out in Section I).
- We note that under Section 3 of Annex A, Committee 6 considered that functions outsourced to unaffiliated entities included "cloud computing services". We wish to clarify whether it is also IOSCO's view, under the Consultation Report, that all cloud computing

services are considered “Outsourcing” regardless of who is providing and consuming the service.

- We believe that “cloud computer services” should not automatically be deemed to be “Outsourcing”, but that an assessment should be undertaken to assess whether such services fall within the definition of “Outsourcing”.