European Association of CCP Clearing Houses

EACH response to the IOSCO Consultation Report "Principles on Outsourcing"

October 2020

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 19 Members from 15 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the IOSCO Consultation Report "Principles on Outsourcing" (hereinafter called "The consultation").

As part of some **general remarks** regarding the Principles on outsourcing defined in the consultation, EACH would like to stress that the importance of outsourcing is constantly increasing, and so is the need for a proper regulatory treatment. We welcome IOSCO's intention to assess the appropriateness of the existing outsourcing principles, particularly as regulated entities are facing a growing number and increasing complexity of regulatory requirements related to outsourcing. This poses a challenge to regulated entities as outsourcing of selected activities has become a widely used tool to handle pressure to reduce costs and enhance efficiency. Moreover, outsourcing allows entities to benefit from new technologies without large one-off investments.

While we support the objectives of the draft principles in general, we consider certain selected aspects of the draft principles as inappropriate or overly burdensome:

- The **definition of "outsourcing" requires further specification** to adequately fit current challenges and recent developments. We consider the proposed definition of outsourcing as inappropriate and not up to date and would strongly support further specifying the definition of outsourcing by limiting it to functions, services activities and processes related to the respective regulated entity's core services.
- Service provision by **dedicatedly authorized service providers should not fall within the scope of outsourcing.** Dedicatedly authorized service providers are subject to supervision by regulators and therefore do not pose comparable risks to outsourcing entities as other unregulated service providers.
- The effectiveness of **intra-group structures should be considered when applying the Principles**. Enforcement along the outsourcing chain can be much more powerful and effectively executed within a group than in the case of a third-party service provider outside such groups. Consequently, those aspects need to be reflected more appropriately especially regarding the requirements on due diligence (Principle 1), concentration risk (Principle 5) and exit strategies (Principle 7).
- Several factors to be considered by the regulated entity when **assessing materiality or criticality are too far reaching or inexpedient**. Factors determining materiality or criticality and requirements to be complied with once materiality or criticality has been assessed should not be mixed. This includes particularly factors related to price formation, investors protection as well as data security and data integrity. Investors protection, price formation, data and information security as well as client's data integrity must always be ensured as required by specific regulatory requirements. E.g.

the mere classification of the data processed as part of the respective outsourced activity does not draw any conclusion on the activity's materiality or criticality.

- The dangers of a strong **market concentration** with a few service providers must be actively countered not only by the regulated entity, but primarily by regulators. Regulated entities should rather be required to appropriately address dependency and concentration risks by ensuring an adequate transfer of services through proper exit management.

Chapter 3 – Fundamental Precepts

Q1. Do you consider the scope of the application of the Principles to entities is clear? If not, why not?

Yes, EACH considers clear the scope of the application of the Principles to entities. However, we believe that IOSCO should explicitly recognize the qualitative differences between a regulated entity outsourcing tasks to an unaffiliated third party and tasks being performed as an intragroup service among affiliates. When tasks are performed as an intragroup service, there is alignment of the interest in the regulated entity in meeting its responsibilities and those performing the tasks because the ultimate shareholders are the same. By contrast, when a third party performs tasks on behalf of a regulated entity there is no such alignment of interests. Importantly, as IOSCO notes, the regulated entity retains full responsibility, legal liability and accountability to the regulator for all tasks.

Q2. Do you consider the concepts used to explain the application of the Principles on Outsourcing to be clear and adequate? If not, why not?

Yes, EACH considers the concepts used to explain the application of the Principles on Outsourcing to be clear and adequate. However, we are of the opinion that particularly the definition of "outsourcing" requires further assessment and specification to adequately fit current challenges and recent developments. While the use of third parties to perform tasks or services has changed considerably in form, scope and number during the past 15-20 years, the definition of outsourcing used to determine the scope of applicability of the principles did not. We consider the proposed definition of outsourcing as inappropriate and not up to date and would strongly support further specifying the definition of outsourcing.

The definition of outsourcing provided by IOSCO serves as the basis for national transpositions and should therefore be defined as a general guiding principle. Based on the current definition as outlined in the "Principles on Outsourcing of Financial Services for Market Intermediaries"[1], many authorities have defined "outsourcing" by including and / or excluding activities (or at least have added such elements to a generic definition) to capture arising challenges and changes in the field of outsourcing. Such approaches are neither clear nor comprehensive. We generally agree with the intended scope of the definition as specified by the examples provided at page 7 of the consultation as well as the definition of service provider used within

[1] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf

the definition of outsourcing. We particularly support the explicit exclusion of purchasing from the scope of outsourcing. However, we are of the opinion that the current definition is not clear enough and misleading.

The wording of the definition of "outsourcing" includes any tasks, functions, processes, services or activities (collectively, "tasks"), which a regulated entity would, or could in principle, otherwise be undertaken by the regulated entity itself. While we generally agree with focusing on functions, processes, services or activities within the definition of outsourcing, we consider tasks as being rather one-time actions that should not be covered by the term outsourcing, although performed by a service provider. The performance of single tasks is generally not related to a transfer of responsibilities to a service provider and should therefore be regarded in line with purchasing.

Moreover, multiple processes, services or activities can be performed by service providers for the benefit of a regulated entity, which are neither specific to the regulated service nor particularly needed in order to perform the regulated services. In case these processes, services or activities are not performed by a service provider, they naturally would be ("otherwise") performed by the regulated entity itself. This is e.g. true for catering, cleaning services, any advisory services or other one-time service. As the term "otherwise be undertaken by the regulated entity" is by far too broad, we would ask IOSCO to limit the outsourcing definition to functions, services activities and processes related to the respective regulated entity's core services. To our understanding this would also include its central control functions (such as Compliance, Risk Management, Accounting and Internal Audit) or such that are required specifically to be maintained by the respective regulated entity (e.g. AML Officer, Compensation Officer). The assessment of materiality and criticality as outlined in Precept F of the consultation report captures this limitation by clearly referring to the ongoing business of the regulated entity. Hence, specifying the definition of outsourcing by referring to functions, services activities and processes related to the respective regulated entity's core services is in line with the assessment of materiality and criticality as well as the clarifying examples provided. In addition, such specification would relieve national standard setting institutions from adding including / excluding examples to provide for an adequate scope of application.

<u>Applicability of the outsourcing principles</u>

We consider the interpretation and implementation of the principles in accordance with the degree of materiality and criticality of the outsourced task as adequate and support IOSCO to further extendm this guiding principle. Although we clearly acknowledge that substantial parts of outsourcing risks also exist in a group context and that the principles should therefore generally also apply to inter-group outsourcings, the "different nature" of intra-group structures should be considered when applying the principles.

Intra-group outsourcings are widely used as they allow for (i) an efficient allocation of resources, e.g. when supplying centralised functions on group level and (ii) the realisation of economies of scale.

The enforcement of outsourcing rules and regulations along the outsourcing chain can be much more powerful and effectively executed within a group than in the case of a third-party service provider outside such groups. Effectiveness of those intra-group structures can be ensured irrespective of the performance of the country of service and irrespective of whether the service provider falls within the scope of the same consolidated supervision. In general, under due consideration of specifics of single group entities, the same standards and policies apply and there is a high likelihood of a common control framework. Further, a reasonable degree of management integration exists, and common committees may be often in place to steer the business and control activities.

In particular, we miss consideration of aspects of group-wide recovery and resolution plans, which clearly capture intra-group outsourcing in a dedicated manner. Capturing risks and additional outsourcing controls in a group context also need to explicitly recognise the principle of proportionality. Consequently, those aspects need to be reflected more appropriately especially regarding the requirements on due diligence (Principle 1), concentration risk (Principle 5) and exit strategies (Principle 7), where we challenge the application in general and ask IOSCO to consider explicit releases for intra-group outsourcings. They are of less relevance or even inappropriate in such a context. We therefore encourage IOSCO to further emphasize the proportional application of the principles under consideration of potential affiliated structures, as already outlined under Section G of the draft principles.

As already stated in our response to Question 1, EACH believes that IOSCO should explicitly recognize the qualitative differences between a regulated entity outsourcing tasks to an unaffiliated third party and tasks being performed as an intragroup service among affiliates. When tasks are performed as an intragroup service, there is alignment of the interest in the regulated entity in meeting its responsibilities and those performing tasks because the ultimate shareholders are the same. By contrast, when a third party performs tasks on behalf of a regulated entity there is no such alignment of interests. Importantly, as IOSCO notes, the regulated entity retains full responsibility, legal liability and accountability to the regulator for all tasks.

Additionally, EACH believes that IOSCO should clearly define outsourcing as an activity that the regulated entity is required to do in conjunction with, or as function of, its regulated activity, and not an activity that the regulated entity could choose to perform. For example, an exchange could choose to clear its members' trades executed on the exchange's platform, but may also choose not to do so, so that such members' trades are cleared by another regulated entity. In this case, EACH would argue that clearing is not considered an outsourced activity for the exchange.

Q3. 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?

We appreciate that IOSCO clearly acknowledges the benefits related to outsourcing, including security related aspects associated with the use of cloud infrastructures. Ensuring information

security, business continuity and disaster recovery often involve the outsourcing of specific elements, which can improve overall security.

We moreover generally share IOSCO's view that outsourcing may pose challenges to regulated frameworks and supervisory authorities and that appropriate limitations in conjunction with appropriate requirements are necessary to limit and manage potential related risk. Notwithstanding this, we would like to point out that extensive minimum requirements and criteria required by supervisory authorities already as of today run the risk of jeopardising any benefits associated with outsourcing, including but not limited to the use of specialist knowledge, the access to new technology and the pooling of knowledge within a group. We are of the opinion that an appropriate handling of outsourcing requires a more focussed approach and should allow for enough flexibility to account for institutions and payment institutions particularities and even more on the particularities of the concerned services, activities and processes as well as the legal framework of operations.

Q4. Does the description of materiality and criticality clearly and adequately address the proportional application of these principles? If not, why not?

We fully agree that the principles should be applied in a proportionate manner, i.e. by considering the relevance of the outsourced service to the regulated entity's ongoing business. However, it is our opinion that several factors to be considered by the regulated entity when assessing materiality or criticality are too far reaching or inexpedient and might conflict with existing national requirements.

We appreciate the simple explanation provided that a "material risk is one that comprises or affects a significant proportion of the tasks of the regulated entity" while "a critical task may be a task that is small in scale but without which the regulated entity is unable to conduct its activities" as it is sufficiently clear and provides appropriate guidance to regulated entities when assessing the materiality and criticality of outsourcing. IOSCO should follow those simple principles when specifying factors to be considered when assessing materiality / criticality.

Although we agree that potential impact on price formation as well as potential negative impacts on clients or on investor protection are of general relevance, we do not consider them as relevant for determining the materiality / criticality of outsourced functions. Preventing harmful price formations as well as ensuring investors protection are usually already covered by other regulatory requirements irrespective of an outsourcing such that it is sufficient to refer to the entities' ability to comply with regulatory or legal requirements as a relevant factor for determining materiality / criticality of outsourced function. Similarly, we suggest excluding the mandatory consideration of the impact on data security and integrity as well as the involvement of critical data for assessing materiality / criticality. Data and information security as well as clients' data integrity must always be ensured as required by specific regulatory requirements on data protection and information security. The mere classification of the data processed as part of the respective outsourced activity does not draw any conclusion on the activity's materiality or criticality.

Moreover, factors determining materiality / criticality and requirements to be complied with once materiality and criticality have been assessed should not be mixed. We do not consider the degree of difficulty and time required to select an alternative service provider or re-integrate the activity as a factor that determines materiality. Rather, proper exit planning ensuring a timely transfer of services should be a regulatory requirement applicable to material or critical outsourcing. There might be services that are being provided by only several highly specialised service providers but do neither relate to the regulated entities' core services nor would their temporary outage result in negative implications. This might, for example, be the provision of internal chatting tools or tools and services related to purchase management.

Finally, we clearly reject obliging entities to analyse and consider aggregated risk exposure due to industry-wide concentration. While we fully acknowledge the potential risk of a high concentration of outsourcings to a limited number of service providers, single entities should not be limited by other entities' choice when selecting the appropriate service provider. It should be the competent or standard-setting institutions' responsibility to manage macroprudential risks. Again, regulated entities should rather be required to appropriately address dependency and concentration risks by ensuring an adequate transfer of services through proper exit management. Requirements to regulated entities outsourcing services related to concentration risk might e.g. be obliged to ensure potential re-integration of those services. Moreover, we would highlight that the operational burden of screening publicly available information to assess potential concentration risk is high and might be misleading due to unavailability of comprehensive data.

Therefore, we strongly suggest deleting the aforementioned factors from the provided list.

Chapter 4 – Outsourcing principles

Principle 1: A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.

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

Yes, EACH considers the Principle adequate and appropriate and generally agrees with the concept that regulated entities should take appropriate steps to ensure they select suitable service providers and that service providers are appropriately monitored, as well as with the due diligence measures proposed. We agree with the measures for implementing suitable due diligence processes and consider them largely as appropriate for selecting service providers but would like to refer to selected aspects which are not sufficiently clear or appropriate in our view.

While we agree that the regulated entity should consider the service provider's ability and capacity to perform the outsourced service prior to entering into a contract with the service provider, it is our understanding that no prior assessment of the service provider's technical, financial, and human resource capacities is required. Rather, should entities investigate

whether there is information available indicating that the service provider might not be able to provide the service as contractually agreed.

Similarly, it is our understanding that ensuring the service provider's compliance with applicable law and regulatory requirements in its jurisdiction does not require the outsourcing entity to assess the laws and regulations applicable to the service provider and its compliance to it. In our view, entities should seek assurance by requesting confirmation of compliance to applicable law. Such confirmation or a separate legal opinion provided by the service provider should also entail a confirmation that there is no applicable law obstructing or frustrating the ability of it or its regulator to obtain prompt access to data. As considered necessary, proof could also be requested in case of material or critical outsourcings as part of an audit.

Moreover, we would like to stress the following: Fundamental Precept "I" requires regulated entities to ensure that sub-contracting is not permissible without the outsourcing entity's prior approval. While we agree with applying the principles along the outsourcing chain in a proportionate manner, we suggest not to require regulated entities to provide explicit approval prior to sub-outsource irrespective to the outsourcing's materiality or criticality. An explicit approval should only be necessary for material or critical sub-outsourcing of material or critical outsourcing. The outsourcing entity should furthermore be free to choose between providing approval of such sub-outsourcing or not rejecting sub-outsourcing notified to the outsourcing entity.

Although referring to Principle 1 under "I", sub-outsourcing is not being further elaborated under Principle 1. Should IOSCO consider including those aspects into Principle 1, EACH would like to ask to respectively amend them before.

Principle 2: A regulated entity should enter into a legally binding written contract with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity

Q6. Do you consider the Principle and implementation measures for establishing the contract with a service provider are adequate and appropriate? If not, why not?

Yes, EACH considers Principle 2 for establishing the contract with a service provider adequate and appropriate. However, EACH is concerned about some of the implementation measures for establishing the contract with a service provider, e.g. (i) guarantees, indemnities, and appropriate types and levels of insurance cover, and (ii) a framework to amend existing arrangements with the service provider, should there be changes in regulatory requirements.

In the context of (i) guarantees, indemnities, and appropriate types and levels of insurance cover, EACH believes that IOSCO should explicitly recognize the qualitative differences between a regulated entity outsourcing tasks to an unaffiliated third party and tasks being performed as an intragroup service among affiliates. When tasks are performed as an intragroup service, there is alignment of the interest in the regulated entity in meeting its responsibilities and those performing tasks because the ultimate shareholders are the same.

In the context of (ii) a framework to amend existing arrangements with the service provider, EACH would agree that having a framework in place to discuss amending existing arrangement with the service provider due to regulatory requirements as sensible and reasonable. However, EACH questions whether it can be reasonably expected from a service provider to contractually commit to address any wholly unknown regulatory changes.

Principle 3: A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.

Q7. Do you consider the Principle and implementation measures for information security, business continuity and disaster recovery are adequate and appropriate? If not, why not?

EACH generally agrees with the Principle and implementation measures for information security, business continuity and disaster recovery, but at the same time would suggest IOSCO to use in the formulation of the Principle the words "evaluate, assess, or consider" (suggesting best practice) instead of the current "ensure" (suggesting a prescriptive requirement), as a prescriptive language could be perceived as being contrary to the fact that, as stated at page 10, the Principles should allow for a risk-based approach.

Q8. 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?"

According to EACH, service providers should ensure that they are capable of providing an unaffected service during business continuity events, such as remote working capacity. Service providers should ensure that remote working practices and procedures maintain the protection of non-public (e.g. client-related) information. It may be a suitable measure to include in the contract that service providers ensure the protection of all such confidential material in any and all business continuity measures or strategies. Ultimately, the same level of access control, redundancy systems and cyber security should be offered and guaranteed regardless of the location of the staff i.e. working onsite vs. working remote.

Principle 4: A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients from intentional or inadvertent unauthorised disclosure to third parties.

Q9. Do you consider the Principle and implementation measures for the management of confidentiality issues are adequate and appropriate? If not, why not?

EACH generally agrees with the Principle and implementation measures regarding confidentiality issues. However, we would like to add that, in Europe, GDPR[2] already provides guidance on provisions concerning information security and personal data protection, and the European Data Protection Board as well as national data protection authorities have already provided guidelines in this regard. Additionally, EACH would argue that enhanced encryption should be consider only for outsourcing to an unaffiliated third party and not be mandated in the case the service is performed as an intragroup service among affiliates.

Principle 5: A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.

Q10. 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?

EACH generally agrees with the Principle 5 measures for the management of concentration risk in outsourcing arrangements adequate and appropriate. However, EACH is concerned about some of the implementation measures. Firstly, we would like to note that risks arising from concentration within the sector need to be evaluated by competent authorities as this is not possible for individual firms.

Secondly, "A regulated entity may also designate a primary and secondary provider. The secondary provider should have the capacity to assume the primary provider's services should an interruption occur." We note that the implementation of Principle 5 does not require a regulated entity to designate a secondary provider and questions the feasibility of having a secondary provider effectively on call/stand-by. Therefore, EACH urges IOSCO to reconsider this implementation requirement for Principle 5.

We consider the requirements related to concentration risk faced by the respective entity – i.e. the risk that multiple material / critical services have been outsourced by the respective regulated entity to one service provider – as generally appropriate. In contrast to this, we consider the requirements related to market wide or systemic concentration risk, i.e. the risk of many regulated entities outsourcing to a single or only few service providers as inappropriate as those exceed the responsibility of single entities and should rather be addressed to competent and supervisory authorities.

We appreciate that IOSCO acknowledges that single regulated entities might not be able to assess whether a service provider serves multiple regulated entity to such extent that it creates systemic concentration risk. Nevertheless, we are of the opinion that the outlined expectations on regulated entities are too far-reaching. Single entities' contribution to managing market-

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

wide concentration risk should focus on risk mitigating measures by requiring regulated entities to maintain reliable exit plans to ensure appropriate transfer of services, either through transfer to on-premise structures or an alternative service provider. Single regulated entities should not be responsible for managing risks created by others by e.g. amending their choice of service providers or underlying contracts (duration), particularly as a change in service provider might be related to a decrease in quality.

The dangers of a strong market concentration with a few service providers (e.g. "lock-in", "data sovereignty" etc.), must be actively countered not only on the side of the regulated entity, but primarily by regulators. Risks arising from concentration within the sector need to be evaluated by competent authorities as this is not possible for individual entities. Also, entities do not know and cannot influence the behaviour of other entities to choose a specific service provider in the sector or in other industries. Furthermore, the consequence of identified concentration risks above a certain threshold by regulators seem unclear. Would an entity be prohibited to outsource services at some point, while others would be allowed ("first come first serve")? This might contradict competition laws and could harm innovation and damage level playing fields.

Principle 6: A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.

Q11. Do you consider the Principle and implementation measures for ensuring access arrangements are adequate and appropriate? If not, why not?

Yes, EACH considers Principle 6 and the implementation measures for ensuring access arrangements adequate and appropriate. However, EACH would like to stress that the supervisory authority should by default first contact the regulated entity. The regulated entity should deliver information to the supervisory authority based on information obtained via requests from the outsourcing service provider.

We consider Principle 6 as not clear enough regarding minimum requirements on access to information for regulators in contrast to outsourcing entities. We agree that outsourcing entities should generally have access to relevant information from the service provider on the provision of the respective outsourced service to fulfil its responsibilities and regulatory obligations. Similarly, regulators might depend on unrestricted access to relevant information related to outsourcing of its supervisory subjects to fulfil its supervisory and oversight function.

Although both, the outsourcing entity and regulators, might depend on information from the service provider related to the outsourcing service, interests as well as the need for obtaining information directly from the service provider might differ and should be reflected in appropriate minimum requirements. Notable, the requirement for outsourcing entities on unrestricted audit and access rights for any outsourcing too far reaching and challenging for non-material / non-critical services. We therefore suggest limiting mandatory contractually

ensured audit rights to critical or important outsourcing only. Regulated entities should in addition be free to decide based on risk assessment whether the reliance on third-party certificates is sufficient to meet their obligation to exercise diligence. Principle 6 should allow regulated entities to suspend the general audit rights as far and as long as the agreed audit surrogates are reliable and delivered in a timely manner. Unrestricted audit rights of regulators could in contrast to this apply to any outsourcing, whereas regulated entities' responsibility related to regulators' access rights should be limited to a proper contractual stipulation. Such approach applies the principle of proportionality in an appropriate manner and reduces costs related to negotiating access rights for non-material and non-critical outsourcings.

Principle 6 moreover explicitly acknowledges the possibility that the outsourced service is performed by a regulated service provider. In such case Principle 6 suggests establishing a cooperation and information sharing agreement between the respective regulators.

We highly appreciate that IOSCO explicitly considers regulated service providers but deems the resulting specifications as insufficient. It is our opinion that services performed by service providers having a dedicated authorisation for performing the respective service should not classify as outsourcing. At least, the outsourcing entity should not be obliged to contractually ensure unrestricted access rights for services performed by regulated service providers in such cooperation and information agreement between regulators is in place.

Finally, we consider the requirement for maintaining appropriate plans for continued access by regulators after termination as not sufficiently clear. Generally, exit plans, to refer to one possible option outlined for fulfilling this requirement, focus on a timely and smooth transfer of services to avoid any disruptions in service provision to the outsourcing entities' clients and less on the availability of potentially relevant information related to the access by regulators. In our view plans to ensure access after termination should first of all only be mandatory for material and critical outsourcings and only in case regulators expressed their need to access information after termination explicitly based on a case-by-case decision. Otherwise service provider might not be willing to enter into outsourcing contracts with regulated entities any longer.

In general, the request for exit plans should be appropriate, as exit plans do often mean significant efforts (i.e. for migrating application and data) and testing may not be possible in many cases. This could be a burden for firms to pick-up the new technology, as e.g. codes would need to be rewritten and retested during operations, which would result in very high efforts.

Principle 7: A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.

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

Yes, EACH considers Principle 7 and the implementation measures for the termination of outsourcing arrangements adequate and appropriate. EACH would argue that the regulated entity should think about the termination of outscoring agreements beyond the strictly contractual aspects and duly consider the next steps while taking account of the materiality and the criticality of the outsourced service. As explained above, EACH believes that IOSCO should explicitly recognize the qualitative differences between a regulated entity outsourcing tasks to an unaffiliated third party and tasks being performed as an intragroup service among affiliates. When tasks are performed as an intragroup service, there is alignment of the interest in the regulated entity in meeting its responsibilities and those performing tasks because the ultimate shareholders are the same. However, termination of an outsourcing agreement between a regulated entity and an affiliate providing intragroup services might prove more challenging and require a more rigorous exit strategy. Therefore, EACH would argue that IOSCO should also explicitly recognize the difference of a regulated entity seeking to terminate an outsourcing agreement for intragroup services with an affiliate.

As already outlined as part of our answer to Question 2, we would welcome a stronger application of the principle of proportionality related to exit planning. We are of the opinion that exit strategies should not be mandatory for intra-group outsourcing. Principle 7 does not consider aspects of group-wide recovery and resolution plans, which clearly capture intra-group outsourcing in a dedicated manner. Group wide enforcement and information structures and processes as well as additional outsourcing controls in a group context should also to explicitly recognise. Further, we consider the requirements on exit strategies as inappropriate for outsourcing of non-critical and non-important functions.

- END -