WORLD FEDERATION OF EXCHANGES

WFE Response to IOSCO Principles on Outsourcing Consultation

September 2020

www.world-exchanges.org

Introduction

We are grateful for the opportunity to respond to IOSCO's consultation report regarding Principles on Outsourcing.

The World Federation of Exchanges (WFE) is the global trade association for regulated exchanges and clearing houses. We represent over 200 market infrastructures, spread across the Asia-Pacific region (~37%), EMEA (~43%) and the Americas (~20%), with everything from local entities in emerging markets to groups based in major financial centres. Collectively, member exchanges trade some $95 trillion a year; while the 50 distinct CCP clearing services (both vertically integrated and stand-alone) collectively ensure that traders put up $1 trillion of resources to back their risk positions.

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair and transparent environment for all sorts of investors and companies wishing to invest, raise capital and manage financial risk.

We seek outcomes that maximise financial stability, consumer confidence and economic growth. We also engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system.

Market infrastructures recognise their responsibilities as critical elements of the financial system, supplying finance to real economy firms and providing a platform for investors even in times of market stress. Accordingly, they had developed business continuity plans, which in recent months have been executed as necessary. This has underpinned what have proved to be record volumes of trading.

In line with its membership criteria and its members' own desires, the WFE has long supported the need for market infrastructures to be prepared and as resilient as possible in the face of a wide range of contingencies. For that reason, over the years the WFE has created working groups, consisting of exchange and CCP experts from across the globe, focused on enterprise and operational risk, as well as on cybersecurity. Operational resilience has been – and continues to be – a priority issue for our membership, and one in which significant time, effort and money has been invested. We therefore welcome the opportunity to offer our perspectives and further contribute to the dialogue, on issues such as outsourcing, in order to secure the shared objectives of fair and orderly markets that promote the safety and resilience of the financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Jonathan Pallant: jpallant@world-exchanges.org
Richard Metcalfe: rmetcalfe@world-exchanges.org

Overview

The World Federation of Exchanges welcomes the general direction of the proposals and recognises the importance of increasing the focus on the resilience of financial services and their third-party service providers, especially in light of the pandemic and the way it has tested the whole ecosystem. The use of principles and a materiality-based approach is particularly important and welcome in providing a guide for the approach of national regulators.

It is important that in terms of operational resilience there is continuity derived from these Principles so that there are not multiple, nor conflicting, disparate sets of jurisdictional requirements that could give rise to a confused and fragmented regulatory environment, especially for those regulated entities operating across borders. Without alignment on the part of national regulators with the fundamental Principles set out by IOSCO, there is a danger that unnecessary administrative burdens will be created, along with additional compliance costs and artificial barriers to trade.

It is also important that common terminology is employed by individual jurisdictions which is consistent with that used by IOSCO and the other international standard-setters. Conflicting language can create confusion and risk, as multiple interpretations arise from different regulated entities seeking to comply with different jurisdiction-specific requirements and terminology.

Given the use of international standards frameworks (i.e. ISO) by regulated entities and regulators, it might be helpful to map or index the Principles in accordance with those internationally recognised standards (to the greatest degree possible), as this would be beneficial in ensuring a common understanding and implementation of the Principles.

Questions

The WFE would provide the following specific commentary in relation to IOSCO's questions.

Question 1: Do you consider the scope of the application of the Principles to entities is clear? If not, wh y not?

The WFE believes that principles, guidance or regulatory requirements relating to issues such as operational resilience, should be all encompassing of the whole financial services industry rather than sectors within it; and led at the international standard-setting body (ISSB) level. 'Levelling-up' the financial ecosystem has clear benefits in terms of reducing the risk of there being a weak link in the chain from end-investor to central market infrastructure. Experience in the second quarter of this year's markets suggests that this is the real issue where operational resilience is concerned.

Levelling-up in a globally co-ordinated manner reflects the global nature of markets and avoids patchwork, siloed approaches and, again, potentially fragmented conflicting future requirements being made by individual jurisdictions. Improving those standards globally is something that benefits the functioning of whole financial ecosystems in serving their national economies. And good order across the ecosystem is only properly served by all parties doing their due diligence in advance, on issues such as outsourcing.

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?

Definition of outsourcing

We are of the opinion that 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 over the last 15-20 years, the definition of outsourcing used to determine the scope of applicability of the Principles has not. We consider the proposed definition of outsourcing as inappropriate and outdated and would 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 appropriately 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 challenges and changes arising in the field of outsourcing. Such resulting approaches are neither clear nor comprehensive.

[1] Principles On Outsourcing of Financial Services For Market Intermediaries, IOSCO, February 2005 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf

We generally agree to the intended scope of the definition as specified by the examples provided[2] as well as the definition of "service provider" used within 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 of outsourcing could be considered unclear and, as a result, unintentionally misleading. In particular, 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". Whilst 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 wholesale by the term "outsourcing", even though they can be performed by a service provider. The performance of single tasks is generally not related to a transfer of responsibilities to a service provider and could therefore, more likely, be regarded as 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 needed in order to conduct their regulated services. In such cases, these processes, services or activities are performed by a service provider, when they normally would be ("otherwise") performed by the regulated entity itself. For example, this is true for any advisory services or other one-time service. As the term "otherwise be undertaken by the regulated entity" is arguably too broad, we ask IOSCO, for the purposes of greater clarity, to limit the outsourcing definition to 'functions, services activities and processes' related to the respective regulated entity's core services. Objectively, we would argue, that this would include its central control functions (such as Compliance, Risk Management, Accounting and Internal Audit) or such functions 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 business activities 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 potentially relieve national standard-setting institutions from needing to include / exclude clarifying examples to provide for an adequate scope of application.

Further, we believe that when using a service provider, which is a dedicated regulated/supervised service provider (e.g. a trade repository, a data reporting service provider, an index provider or a CSD), that the use of them should not fall within the scope of outsourcing in the same manner as other forms of service providers, irrespective of whether the provision of that specific activity requires explicit authorisation or could also be performed by the regulated entity itself. Such dedicated service providers are subject to supervision by regulators and therefore do not pose risks comparable to outsourcing to unregulated service providers. Instead, greater emphasis should be placed on cooperation and information sharing arrangements should be established with the regulator of said regulated service provider, as suggested as part of Principle 6.

Applicability of the outsourcing principles

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 extend 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 intra-group outsourcings, the effectiveness of intra-group structures should, we believe, be further 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 at a group level and (ii) the realisation of economies of scale.

[2] Principles on Outsourcing - Consultation Report, IOSCO, May 2020

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 operating outside such groups. Effective control structures are ensured by intra-groups, irrespective of the country in which the service provision is conducted and irrespective of whether the service provider falls within the scope of a different regulatory authority. In general, the same standards and policies apply as under single entity supervision but there is also a high likelihood of a common control framework being employed by intra-group entities, strengthening those controls. Further, a reasonable degree of management integration exists, and common committees may often be in place to steer the business and control activities.

We would advise that there is the potential to miss the additional beneficial considerations arising from group-wide recovery and resolution plans, which clearly capture intra-group outsourcings in a dedicated manner. In capturing the risks and additional outsourcing controls in a group context, the explicit recognition of the principle of proportionality is also needed. Consequently, those aspects may 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 exemptions for intra-group outsourcings. This is on the basis that they are of less relevance or even inappropriate in such a context and would be unduly burdensome.

We therefore encourage IOSCO to further emphasise proportional application of the Principles under consideration of potential affiliated structures, as already outlined under Section G of the draft Principles. The required due diligence processes within a group entity should offset concerns around the potential for perceived lack of independence or conflict of interests, and it is the ultimate responsibility of the regulated entity to make appropriate governance and due diligence arrangements.

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?

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 involves the outsourcing of specific elements, which has the potential to actually improve overall security.

We 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 highlight the general point that extensive minimum requirements and criteria required by supervisory authorities, even in their current form, could run the risk of jeopardising the 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 focussed approach and should allow for enough flexibility to account for the particularities of the concerned services, activities and processes, as well as the legal framework of operations. In general, we encourage enabling the most appropriate form of flexibility for entities to tailor their own risk-based approach to managing the outsourcing process, as prescriptive requirements can quickly become outdated especially, for example, when overseeing technology service providers.

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

The WFE notes that, included amongst the factors for the materiality and critically assessments is: "*Aggregated risk exposure due to industry-wide concentration of outsourced material or critical services to the same provider, where the regulated entity is aware of this, or is reasonably able to determine this from publicly available information.*"

As implied in the text, given the confidential nature of critical services being provided by service providers, this factor would be difficult to assess and may create an obligation that is unlikely to be answered or to result in meaningful risk mitigation. International standard-settings bodies (ISSBs) and regulators would be better placed to give consideration to industry-wide concentration risk issues rather than individual market infrastructure firms. That engagement might be best served via reviewing those providing Infrastructure as a Service (IaaS) for a material amount of a market and to systemically important financial service firms.

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

We agree with the measures for implementing suitable due diligence processes and consider them to be appropriate for selecting service providers in large part. However, we would like to point to specific 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. Indeed, it is often only whilst formally engaged with service providers that entities would be able to access and fully investigate specific information.

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 through requesting confirmation of compliance to applicable law. Such confirmation or a separate legal opinion, should be provided by the service provider.

Moreover, we would like to point to 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 that regulated entities are not required to provide explicit approval prior to sub-outsourcing. An explicit approval should only be necessary for material or critical sub-outsourcings of material or critical outsourcings. The outsourcing entity should furthermore be free to choose between providing approval or 'not rejecting' the sub-outsourcings notified to the outsourcing entity.

Although referring to Principle 1 under Precept "I", sub-outsourcing is not further elaborated under Principle 1. Should IOSCO consider including those aspects into Principle 1, we request that they are amended respectively prior to inclusion.

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 generally reflects the awareness that the level of detail of the written contract –"which should reflect the level of monitoring, assessment, inspection and auditing required, as well as the risks, size and complexity of the outsourced services involved." However, many service providers, especially for cloud-based services, offer a "one-to-many" service model, meaning service is provided in the same way to many different customers. As a result, service providers generally offer the same or substantially similar contract terms to those different customers without the flexibility to have bespoke arrangements. In addition, many requirements – particularly technical, operational, and functional requirements – are not addressed in the terms of the contract, but in the service provider's policies and procedures, third-party audits, certifications, and governance practices. Thus, a regulated entity must consider and address the elements of outsourcing not only by way of the contract with the service provider, but also through a review of those policies, and procedures, third-party audits, etc.... For example, a firm may decide not to outsource certain obligations related to records management or encryption key management. In these situations, the written legal agreement would not directly address those functions, though it would be the regulated entity's responsibility to explain its arrangements to competent authorities.

The Principles and *implementation* measures could be amended to better reflect that a regulated entity can meet the Principles through a robust due diligence process and a complete governance programme, and not only via reliance on a contract.

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?

Ensuring the ability for all market participants to ingrain resiliency-based measures in their organisations is fundamental to the need for an ecosystem-wide approach to operational resilience.

Prior resilience measures were integral in shielding market infrastructures in relation to pandemic related threats, such as the use of phishing emails (in a remote working environment, which did not in practice represent a new form of attack but simply had altered content or 'bait' relating to Covid-19 related matters). In other words, whilst Covid-19 has been a practical, specific example of why good operational resilience is important, it highlights that operational resilience measures are a prerequisite to ensuring the continued functioning of an organisation, following an incident or event, and that the pandemic in itself should not radically alter the general approach to managing resilience. Achieving the end outcome of operational resilience, and recognising the existing measures in place, should be kept in mind when considering any additional or further guidance in the wake of the analysis of the impact of the pandemic. The WFE has separately detailed the type of cyber-resilience measures that were scaled-up by its members[3] in response to the pandemic and the need to have mass remote working.

In seeking assurances in any due diligence process with third-parties, it might be helpful that, where a vendor is regulated (either directly or as part of a corporate family), information necessary to evaluate the third-party should also be permitted to come from the vendor's home country regulator. This may be particularly relevant following the experiences between firms and their vendors over the pandemic, where there is an extent to which an individual

[3] The World Federation of Exchanges publishes update on industry cyber efforts during the pandemic, May 2020, WFE https://www.world-exchanges.org/storage/app/media/WFE%20Update%20%20How%20Market%20Infrastructure%20is%20delivering%20Safe%20and%20Efficient%20Trading%20Venues%20during%20a%20Global%20Pandemic.pdf

firm is necessarily limited in how it can oversee its third-parties and be privy to all apposite information. For instance, this may have arisen when on-site inspections could not occur due to social-distancing restrictions and remote working arrangements.

A supplementary approach to issues concerning the business continuity of a regulated entity's vendors and managing mass remote working, or extreme situations more generally, may be to give greater focus (whilst recognising their existing inclusion) on ensuring that the contingency planning process incorporates appropriate exit strategies.

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?

While the Principle for this action is adequate, the implementation may not be appropriate for the regulated entity. Similarly to question 4, the assessment of concentration risk of a service provider across the industry would be difficult to achieve and create an obligation that may not result in risk mitigation. Systemic risk related to a single provider may be best governed and overseen by regulatory authorities, duly backed by the standards set by ISSBs.

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

All instances of "ensure" (which suggests something within the regulated entity's direct control) in Principle 6 should be modified to "evaluate, assess, or consider" (suggesting monitoring of the performance of third-parties). This change in the text would implicitly recognise that regulated entities may achieve the goal of access to service-provider information for the regulated entity and regulators either directly, indirectly, or through reliance on "pooled audits or assurance statements".