WORLD FEDERATION OF EXCHANGES

WFE Response to the FSB's Discussion Paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

December 2020

www.world-exchanges.org

Introduction

We are grateful for the opportunity to respond to the FSB's Discussion Paper on *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*.

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.

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

Questions

1. **What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?**

Managing and mitigating the risks relating to outsourcing and the use of third-parties, as well as the broader supply chain, has been a key priority and area of intense focus for market infrastructure firms. This work began long before the pandemic as market infrastructures use third-parties/outsourcing to better serve customers by employing the new technologies or services they offer (which may not otherwise be feasible for the market infrastructures to provide in their own right). Market infrastructures are acutely aware that the use of third-parties/outsourcing must be undertaken in a safe and efficient manner and not compromise their operations. The pandemic has seen an additional focus from market infrastructures on long-term strategies (eg, enhancing communications/engagement with third-parties via new mechanisms) for the use of third-parties/outsourcing, to ensure safe and efficient service provision.

Market infrastructure firms do not subscribe to the notion that the use of third-parties or outsourcing enables the 'outsourcing of responsibilities'. Actively working to deliver safe practices in the use of third-parties/outsourcing is integral to a financial institution's franchise (ie, its business model) and reputation. However, to avoid restricting the benefits associated with third-parties/outsourcing, there is a need to ensure that reasonable requirements (ie, readily achievable resourcing implications) and expectations are made by regulators in relation to a financial institution's oversight of their third-parties/outsourcing. Avoiding a series of prescriptive definitions and requirements that differ from one jurisdiction to another is also important to avoid static, untailored requirements for evolving threats that do result in beneficial outcomes for resilience. Instead, a risk-based and outcomes-focused approach presents a more agile way of addressing operational risk and resilience related issues, given their evolving nature. This is particularly relevant in enabling firms to deliver a high-standard of oversight across their third-parties/outsourcing but with a tailored approach that reflects the degree of criticality and dependency (by the financial institution on the third-party to support the delivery of functions/critical functions) of the service provided (ie a regulated activity). For instance, the extent to which 'mapping' is required can be guided by such considerations. Such an approach would also lend itself to supporting a more harmonised cross-border approach to third-parties/outsourcing regulation and supervision, via the greater use of deference.

The FSB paper refers to both third-parties and outsourcing in combination. Often the two are conflated; improved and standardised definitions for outsourcing and third-party relationships may be appropriate. The FSB's paper highlights the varying nature of these definitions between national regulators and standard-setting bodies[1].

Regarding the definition of 'outsourcing' (regulatory scope), we believe it will be important to consider a definition which enables a risk-based and balanced approach. For example, we generally agree to the intended scope of IOSCO's definition (cited in the paper) and welcome the work to provide core guidance in this field but are of the opinion that the definition could be unclear and inadvertently misleading.

IOSCO's definition of "outsourcing" involves a regulated entity using a service provider for any tasks, functions, processes, services or activities (collectively, "tasks") which would, or could in principle, be undertaken by the regulated entity itself. While we generally agree with focusing on "functions, processes, services or activities" within

[1] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, FSB, November 2020, Pg. 17-18

the definition of outsourcing, we consider "tasks" as being rather one-time actions that should not be covered by the term "outsourcing", albeit 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" (which is excluded from the scope of this definition of outsourcing).

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, and in considering this particular definition, it would be helpful for the purposes of clarity to limit the outsourcing definition to 'functions, services, activities and processes' related to the respective regulated entity's core services.

When dealing with a third-party service provider, which is a regulated entity (eg an exchange, CCP, trade repository, a data reporting service provider, an index provider, benchmark administrator, investment firm or a CSD), the provision of regulated services ought not to fall within the scope of third-party regulatory oversight requirements in the same manner — irrespective of whether the provision of that specific activity requires explicit authorisation. This should also apply when the provision of that activity could 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 the use of third-parties/outsourcing to unregulated service providers. It would be unrealistic for financial institutions to conduct comprehensive oversight of such regulated entities, especially where they are a necessary (sometimes under other regulatory requirements) part of a regulated value chain.

Identifying and managing fourth-parties/subcontractors used by third-parties/outsourcing may pose practical challenges. The WFE welcomes the FSB's recognition of these challenges posed by certain supply chains and notes with interest the approach of the South African Reserve Bank[2] in this regard. The use of technology to assist in this process, coupled with existing thorough application of third-party risk management (TPRM), are important components that market infrastructure firms continue to explore. The WFE believes it is highly beneficial for regulators to work with firms in taking advantage of such technologies to achieve greater resilience and oversight of the supply chain. The WFE would also highlight the practical challenges that arise, for firms, from performing oversight for fourth-parties or subcontractors and that greater benefit could be derived from regulators instead having a focus on implementing principles-based requirements that permit reasonable approaches, such as contractual provisions requiring pre-approval of a sub-contractor performing critical services and/or contractual provisions that limit sub-contractors to those that have received a specified independent review or certification.

Ongoing cyber threats to all companies remain a concern and the prior implementation of cybersecurity measures has helped market infrastructure firms in combating that threat. As a universal threat to the ecosystem of financial services, the WFE publicly shared a report on some of the measures undertaken by its membership earlier in the year[3].

The pandemic also posed additional complications to operating practices which market infrastructure firms faced and mitigated. This is discussed in response to question three and four.

[2] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, FSB, November 2020, Pg. 24
[3] The World Federation of Exchanges publishes update on industry cyber efforts during the pandemic, WFE, May 2020

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

As previously mentioned, the WFE recognises that there has been and continues to be a growing use of third-party/outsourcing providers by market infrastructures. Their use is often to improve efficiencies or effectiveness, to reduce exposures via specialist/expert providers, to better serve customers by employing new technologies and to enable forms of service provision which would not otherwise be feasible or viable. Often the reasoning behind the use of third-parties is to address those objectives that in part this consultation is seeking to review – ie, improving resilience and mitigating risks. It is, of course, only right that care is taken in the selection and use of such providers and this remains a priority for the WFE's membership.

It is also widely understood that where a third-party is providing a 'critical or important operational function', on which an organisation is in practice reliant, that in particular there is appropriate due diligence in place. Firms are in the best position to identify the scenarios and testing necessary for their third-parties/outsourcing. However, whilst members of the WFE undertake thorough and extensive TPRM, some regulations may represent unnecessarily burdensome and resource intensive testing and scenario planning of a third-party provider—for example, requiring vast numbers of severe/extreme but plausible scenarios to be worked through. This would be especially so where there are excessively loose parameters placed on the scope and breadth of those scenarios by regulatory authorities.

This is not to advocate the *removal* of accountability with financial institutions but rather to flag that there is potentially a heavy resource implication associated with such additional regulatory and contractual requirements needing to be embedded in firms' TPRM, such as testing processes and audit. These may be sizeable and may have implications for the firms in the aggregate cost benefit analysis. However, if regulatory authorities were to enable financial institutions to appropriately collaborate, or were to facilitate solutions for, applying robust TPRM whilst avoiding unduly burdensome requirements it would naturally be beneficial for all parties. For example, the responsible use of 'pooled audit' may lower the operational overhead experienced by both parties (especially for firms with many counterparties or clients).

Ensuring that there are reasonable expectations by regulators of financial institutions is also an important consideration in itself. Whilst firms must work to be ever more resilient in their practices with third-parties/outsourcing, the expected application of risk management measures should be manageable and proportionate. For example, when discussing risk measures relating to an outsourced/third-party service provider, eg a cloud provider, it is unlikely to be economically or practically feasible to run a live back-up system, either through an additional third-party or in-house to the same level as the primary provider. Instead, a reasonable focus would be on the use of appropriate exit strategies. Avoiding unachievable measures being left as 'open' requirements on financial institutions (possibly exacerbated through opaque or too broad a use of language when a regulator is in effect setting specific requirements) would be beneficial in helping both financial institutions and regulators achieve thorough and consistent TPRM. Where there is a lack of clarity for existing specific regulatory expectations, alongside unwieldy and vast sets of requirements, it potentially inhibits the financial institution as it draws unnecessary resources and inadvertently could generate conflict between a financial institution and regulator as those expectations cannot be met.

A form of standardisation of due-diligence requirements, ideally set at the international level, would also be beneficial in delivering greater transparency, certainty and provide a cross-border footing for global business to use third-parties in a safe and efficient manner – whilst ensuring that they meet regulatory requirements. This would be particularly helpful for managing risk assessments or, for example, the concept of 'standardisation' might extend to the use of third-party/outsourcing contracts. A form of 'master agreement' might be worth consideration in its

potential practical application to overcome some of the difficulties and challenges arising from meeting regulatory requirements when a financial institution is forming a legal agreement with a third-party provider. Often those requirements may include stipulating what should be addressed in the third-party legal contract. This can conflict with the contractual terms laid out by tech providers when they often are offering only common/default contractual terms. Having a master agreement might avoid such conflict and be especially helpful for SMEs, who may not have much leverage for negotiating their contract. By generating a form of master agreement, akin to the role that the ISDA Master Agreement plays in OTC derivatives,[4] but for third-parties/outsourcing, it may also mitigate the need for jurisdictions to set out their own approaches and an associated unhelpful 'patchwork' of rules subsequently emerging. Such an approach may also help to ensure that third-party/outsourcing contracts are providing the necessary transparency to quickly determine if they are reaching regulatory expectations – providing certainty to all signatories and reducing the regulatory burden on businesses.

The WFE welcomes a balanced approach to intra-group outsourcing related regulation. The safe and efficient application of regulation to intra-group outsourcing is greatly benefited by proportionate and balanced requirements that do not create unnecessary burdens and duplications that ignore the efficiencies that can safely be derived from the use of intra-group outsourcing. The cited approach of the Bank of Italy ("a group can be deemed as a single economic entity" and "the power of direction and coordination of the parent undertaking"[5] in intra-group situations) and the nuanced approach[6] of the German regulatory authorities are both supportive examples of such a balance.

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

There may also be cross-border implications for TPRM resulting from rules or restrictions imposed by a home-country or home-country regulator. For example, it may not be possible for on-site audits to be conducted at the third-party and there may be instances where certain reports include confidential supervisory information that could not be shared externally without approval. The level of protection extended to intellectual property can also vary across jurisdictions. These complexities create challenges, increase costs, and can be burdensome for financial institutions. 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 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 testing of multiple vendors and, for example, managing extreme scenarios, could focus on ensuring that the contingency planning process incorporates appropriate exit strategies.

It is important that any proposed third-party/outsourcing requirements can be implemented, or are compatible (as far as possible, recognising that local authorities are most familiar with the unique characteristics of the firms they supervise and the legal framework under which they operate), globally and by all sectors in the ecosystem. This could be coordinated and achieved at the international level while, again, balancing the importance of local

[4] A standard contract used for all over-the-counter (OTC) derivatives transactions entered into between the parties.
[5] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, FSB, November 2020, Pg. 20
[6] Allow the establishment of specific processes to "be waived in the case of outsourcings within a group or within a network of affiliated FIs" on proportionality grounds, Ibid, Pg. 28

supervisory authorities retaining their autonomy in adopting regulatory requirements for the firms they oversee. Indexing regulatory requirements to common standards would also aid the process. Such an approach would help to avoid inadvertent fragmentation and needless differing/conflicting regulatory expectations and requirements applying in different jurisdictions. To ensure these aims, the WFE encourages the FSB to continue to co-ordinate their members third-party/outsourcing related requirements, as well as continuing to liaise with their public and private sector stakeholders, with the aim of producing a more globally coordinated and consistent approach. A harmonised and coherent approach is particularly relevant for all future operational resilience related initiatives, given the potential for additional jurisdiction specific legislation and regulatory requirements to emerge in response to the pandemic. Conflicting practices risk regulated entities needing to implement multiple sets of requirements, adding to the risk of confusion and inefficient implementation (especially when the pandemic threat is still live).

Further, it is important that the regulatory approach, driven by international standard-setting bodies (ISSBs), is one that is based on outcomes-focused regulation to enable a strategic approach to ensuring protection against risk. In the absence of such an approach, a regulatory patchwork is also likely to continue to evolve. Whilst there are common principles across some jurisdictions[7], firms are currently being faced with numerous prescriptive compliance requirements (especially in relation to the use of new technologies) that can differ from country to country – unnecessarily absorbing resources. This is coupled, in some jurisdictions, with opaque language about what are existing specific regulatory expectations that financial institutions will be measured against. Achieving a common, outcomes-focused approach, via enabling mutual recognition or other forms of deference[8], should avoid an uncoordinated regulatory environment developing but with appropriate accountability remaining with market infrastructures as regulated financial institutions. The WFE welcomed IOSCO's efforts in providing core guidance around the use of outsourcing[9], as well as the FSB's survey analysis, and would support further efforts to achieve this aim at the international level.

There is also an understandable focus by regulators on addressing the issue of concentration risk. Market infrastructures have recognised these risks and strive to avoid single points of failure, coupled with appropriate risk mitigation measures (eg preparing appropriate exit strategies). However, recent proposals have come forward from some quarters that may not be practical nor will assist with addressing concentration risk in an achievable or meaningful way. There is a natural limit to which market infrastructures can diversify their third-party relationships when there are certain, necessary, providers required as part of the value chain, which unavoidably results in some concentrations of use by financial institutions. Another emerging discussion around requirements for financial institutions is to identify where the firm/group is using a third-party/outsourcing that would present a concentration risk due to equivalent financial institutions also using that vendor. While it is reasonable and desirable for a firm or group to consider its own degree of concentration risk vis-à-vis a given third-party, it is not clear how in practical terms such a financial institution could ascertain how many of its peers are also using that same third-party. Third-parties are typically restricted by contract from disclosure of other firms' use of the services. 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, for example, those providing

[7] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, FSB, November 2020, Pg. 1

[8] The role of appropriate regulatory deference in laws and rules related to operational resilience in the use of third-parties/outsourcing is worthy of careful consideration. Often the proposals so far outlined by individual jurisdictions include thorough, resource intensive work (eg BoE Operational Resilience, 2019) to be undertaken to satisfy the requirements. Further, if each national jurisdiction were to continue to make analogous requirements for unnecessarily differentiated work, to achieve similar outcomes, the result would be unduly burdensome for globally active firms. The FSB's discussion paper is beneficial in outlining much of the 'state of play' in this regard and we believe could be a platform for consideration to be given to how these requirements might operate in terms of deference and mutual recognition for cross-border arrangements.

[9] Principles on Outsourcing, IOSCO, May 2020

Infrastructure as a Service (IaaS) for a material amount of a market and to systemically important financial service firms.

It is understandable that avoiding concentration risk and enabling greater scrutiny of third-parties/outsourcing is desired by the regulators. Recent regulatory proposals have also raised the prospect of restricting the use of third-parties/outsourcing when it is provided from a vendor based or operating from a third-country/overseas. Within the context of the general use of third-parties/outsourcing, prohibiting access to third-country/overseas providers (such as ICT providers) may instead create more risk and reduce the resilience of financial institutions. Given the 'niche' services that market infrastructures (or other elements of the financial services ecosystem) can require, there is often limited service provision that can meet the stringent high-standards of resiliency requirements that market infrastructures demand of the third-party service providers they employ. By reducing access to that list of service providers, greater concentration risk could occur and less tested and robust service providers might instead be used out of a lack of choice rather than on the basis of resiliency, suitability and merit. Introducing such restrictions (for example, on the basis of requiring access for onsite inspections for jurisdiction-based regulators) may have unintentional additional consequences, such as forms of data localisation. There is also the base question of whether such a severe form of restriction is proportionate to the risk that use of an overseas third-party would create.

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

As previously mentioned, in seeking assurances in any due diligence process of 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 that third-party may be obtained directly from the vendor's home-country regulator (supported as necessary by MoUs and multilateral MoUs). This would also remove unnecessary burdens on the regulated entity, while ensuring transparency into the activities of third-parties, as far as possible, and potentially in their use of any fourth-parties/ broader supply chain.

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 to ensuring that a financial institution's contingency planning process incorporates appropriate exit strategies.

The pandemic also highlighted some of the benefits associated with the use of third-parties/outsourcing, such as improving aspects of risk mitigation through greater geographical spread of a firm's providers. This gave firms time to adjust contingency planning as the impact of the pandemic varied in its effect on different regions and over different time periods.