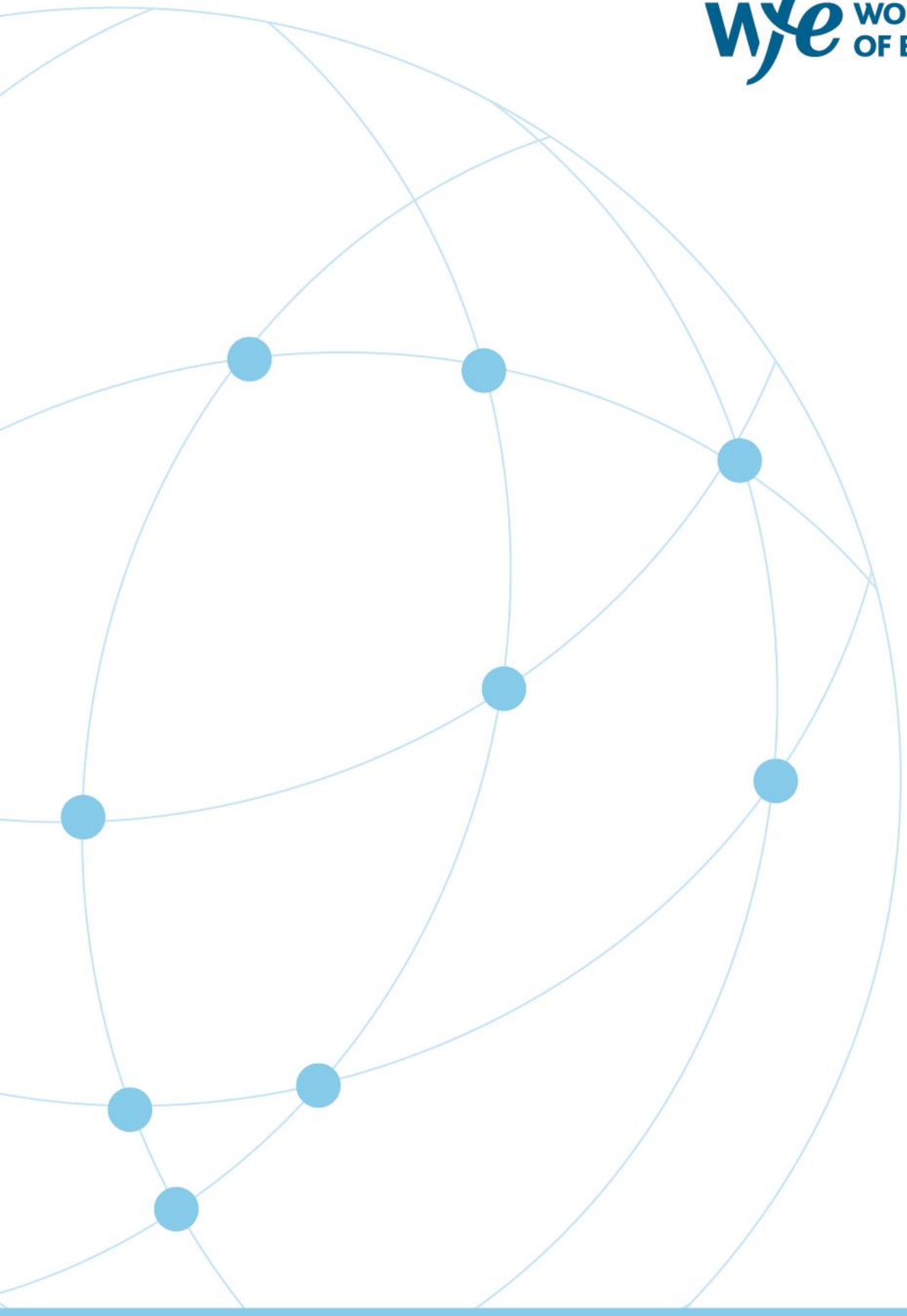
WORLD FEDERATION OF EXCHANGES



FSB – enhancing third-party risk management and oversight

22nd August, 2023

Background

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents over 250 market infrastructure providers, including standalone CCPs that are not part of exchange groups. Of our members, 34% are in Asia-Pacific, 45% in EMEA and 21% in the Americas. WFE's 90 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. WFE exchanges, together with other exchanges feeding into our database, are home to over 50,000 listed companies, and the market capitalisation of these entities is over $100 trillion; around $140 trillion in trading annually passes through WFE members (as of end-2022).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policy makers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally 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:

James Auliffe, Regulatory Affairs Manager: jauliffe@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

or

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org.

Response

Overall comments

The WFE welcomes the opportunity to respond to the FSB's consultation on enhancing third-party risk management and oversight. We value the way the FSB has been open with stakeholders in the formation of this work and look forward to further discussions with the FSB and its members. We appreciate that the FSB took a risk-based approach that focuses on critical services, as determined by each financial institution individually. We also appreciate the flexible nature of the toolkit, allowing each financial institution to design their TPRM programmes tailored to their needs and relationships. Before turning to our specific responses, we are setting out our overall thoughts on third parties and risk management of them.

As they have for many years, businesses can rely on third-party providers to support their operations and achieve their goals. Financial institutions are no exception, as they engage with third parties to perform various functions, such as technology support, legal services, and data management. Third-party relationships can play an important role in the smooth functioning of their services.

Using third parties can help financial institutions to potentially lower costs and produce higher quality services through a variety of means, including management of risk.

One of the key benefits of using third parties is access to specialist expertise and services. This is particularly important when considering the enterprise risk management and operational resilience of financial institutions. Financial institutions face numerous risks and, depending on how the financial institution employs third parties, they can potentially help to manage these risks. For example, rather than solely testing their cybersecurity systems themselves, financial institutions may employ third parties to test them as well. One potential benefit of using external party testing of a financial institution's cybersecurity programme is that the third-party may use a broader framework for testing so they may find gaps that otherwise would not be found, leveraging their broad industry knowledge.

Moreover, another potential benefit of using third parties can be to provide access to capabilities and facilities to financial institutions in a more efficient manner than if they provided the capabilities and facilities on their own. This is particularly true for smaller financial institutions, which may not have the resources to invest in the latest technology or infrastructure. Broadly, depending on the size of the financial institution and the third-party service being provided, outsourcing to third-parties can provide additional flexibility and agility.

When we discuss third parties, we should not only consider the risks that they bring, but also the innumerable benefits that they bring to risk management and other aspects of running a financial institution; and, ultimately, the overall goals of policy-makers around the world – economic growth, financial stability, market integrity, innovation, and good outcomes for consumers.

Chapter 1

1. Are the definitions in the consultative document sufficiently clear and easily understood? Are there any important terms and definitions that should be included or amended?

We appreciate the FSB's recognition that differences in regulation and industry practices exist across jurisdictions and thus, "complete harmonisation of terms is not always possible or desirable." Along these lines, the WFE also appreciates that the definitions proposed by the FSB are intended to be simple and clear.

While the definitions are generally reasonable, it is important for local policy-makers and individual financial institutions to continue to be able to leverage within their own regulatory frameworks and policies, respectively, definitions that are appropriate for the institutions they oversee and services they offer. Therefore, in recognition that it may be difficult to have common definitions across regulatory regimes, WFE recommends best practices be applied that provide flexibility for a financial institution to act in accordance with its risk management practices. Every institution should have flexibility to tier their third-party providers based on usage and the role that provider plays. Along these lines, WFE cautions against a common definition for "systemic third-party dependency", as each financial institution should identify what is critical for its organization, and systemic impact should be a part of that definition, not separate.

WFE also has a technical comment with respect to the FSB definition of outsourcing, which is proposed to be defined as "*A category of third-party service relationships where a financial institution uses a service provider to perform, on a recurrent or an ongoing basis, services, or parts thereof, that would otherwise be undertaken, or could reasonably be undertaken, by the financial institution itself."*

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 performed by the regulated entity itself. For example, this is true for any advisory services or other one-time service. As the term "could reasonably be undertaken" 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 regulated entity providing its core services.

Chapter 2

2. Are the scope and general approaches of the toolkit appropriate?

We welcome the FSB's proposal to generally not consider "regulated financial institutions, to the extent they are engaging in financial services transactions, such as correspondent banking, lending, deposit-taking, provision of insurance, clearing and settlement, and custody services" as third-party service providers. We appreciate the FSB's recognition that such institutions are already subject to comprehensive supervision and regulation by their respective local regulators.

The focus should be on prioritization, resilience, and risk reduction, and the cost/benefit of using certain tools in the toolkit should be considered. Some of the tools may increase day-to-day risk for financial institutions while decreasing tail risk, and financial institutions should have flexibility to employ tools from the toolkit based on their overall framework.

3. Is the toolkit's focus on regulatory interoperability appropriate? Are there existing or potential issues of regulatory fragmentation that should be particularly addressed?

Yes, the toolkit's focus on regulatory interoperability is appropriate and a key area of focus amongst WFE members. WFE appreciates the FSB's recognition that legal differences between regulatory and supervisory regimes exist across

jurisdictions as do different business models within financial institutions. In line with WFE's comments above, it's important that jurisdictions and financial institutions be able to adopt TPRM and operational resilience requirements and programmes that are tailored to their unique needs.

As such, we would like to emphasise the importance of the FSB's toolkit adhering to the FSB's intended objective, as it states, of "setting out aligned and comparable, outcomes-based frameworks to manage third-party risks, while avoiding a one-size-fits-all approach that does not permit differences in regulation or market structure."

Additionally, where financial institutions are designated as critical national infrastructure, they may be reporting to a national protection authority, as well as being subject to regulation and supervision by a financial services regulator, potentially, even multiple in different jurisdictions. We recognise that national protection authorities are outside the purview of the FSB, but we would welcome a statement encouraging greater co-operation between national protection authorities and financial regulators in order to achieve greater coordination. Moreover, we would encourage greater information sharing between these types of authorities to prevent duplicative reporting and requirements.

Broadly, conflicting or multiple requirements are challenging for financial institutions as they leave them having to comply with multiple varying requirements. To that end, the WFE also supports the FSB's intention to achieve greater convergence across the regulatory requirements. We hope that the proposed format for incident reporting exchange model is the start of a process that will ultimately lead to fewer conflicting or multiple requirements and lower reporting costs.

4. Is the discussion on proportionality clear?

The WFE supports risk-based and proportionate approaches being taken with respect to a financial institution's third-party relationships. Each financial institution must be able to independently determine which third-parties are critical service providers to its operations and approaches of proportionality should be applied along those lines. For example, as stated in the report, while a service provider may be critical to one financial institution, this may not be case for another financial institution.

In line with this, the WFE challenges the assertion that "[t]he failure or disruption of a critical service may have a greater impact on financial stability if it affects larger, more complex financial institutions, which in turn warrant stricter regulatory expectations and more intensive supervision." Whilst we recognise the theoretical risk of a greater impact on stability if a larger financial institution is involved, the likelihood of impact is most likely lessened by the increased resources larger financial institutions are able to commit to risk management. As recent cyber events (eg, ION, MOVEit) have shown it is more likely that disruption is caused through smaller entities. Regardless, as long as proper risk mitigation techniques are in place, as there were in recent events, the risks can be managed in a way that ensures relatively smooth functioning of the financial system. The FSB could re-draft to say that "[t]he failure or disruption of a critical service may have a greater impact on financial stability if it affects ***and is unmitigated at*** larger, more complex financial institutions, which in turn warrant stricter regulatory expectations and more intensive supervision."

Ensuring that there are reasonable expectations by regulators of financial institutions is important. Whilst financial institutions must work to be ever more resilient in their practices in managing the risks and interruptions arising from third parties, the expected application of risk management and resilience measures should be manageable and proportionate. For example, when considering risk measures relating to a cloud services provider, it is not necessarily 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 other practices employed by the

financial institution to effectively mitigate and manage the associated risks (eg, use of appropriate contracting provisions and exit strategies).

As another example, the WFE suggests additional proportionality be applied related to nth-party risk. For example, it is unrealistic for smaller financial institutions to know who all the nth-parties are, given resources. It is also challenging for large financial institutions, because they may have many third (and therefore nth) parties and many third parties are reluctant to provide the identity and other information on their own third parties. There is a limit to how far financial institutions could reasonably go given that their contractual arrangements are with their third-parties and not the nth party. In addition, ongoing maintenance of nth-party lists should be considered, given impact on TPRM programmes and resources.

Chapter 3

5. Is the focus on critical services and critical service providers appropriate and useful? Does the toolkit provide sufficient tools for financial institutions to identify critical services? Do these tools rightly balance consistency and flexibility?

In line with our comments above, we welcome the focus on critical services and critical service providers, as this allows financial institutions to comprehensively manage their risks, while focusing on mitigating and managing the risks that arise from the service providers that are most critical to them individually. We appreciate that the FSB recognises that financial institutions are usually best placed to assess the criticality of services they receive or plan to receive because relationships with third-parties vary across financial institutions.

Nevertheless, we consider it too rigid to state that "third-party service relationships involving the provision of critical services from service providers should include an assessment of potential benefits and risks and be approved by the board, senior management or an appropriate body of the financial institution." We agree that there ought to be proper oversight and governance of an FI's TPRM framework but approval by the board for individual third-parties is too prescriptive.

Notably, financial institutions' risk assessment and management of third-party risks is generally conducted on a graduated scale. Financial institutions typically assess risks of an event or risks related to a third-party in a variety of ways, but common practice uses a scale based on the degree of risk, often related to the likelihood and impact of failures or incidents. Financial institutions apply differing risk mitigating tools and resilience strategies depending upon the level of risk identified and criticality to the institution.

It is generally accepted practice in enterprise and third-party risk management to develop assessment scales that rank the impact and likelihood of a risk event and/or service. We could take impact to be synonymous with criticality here. In a typical example, the highest impact risk event could be severe and given a risk rating of 5 and a low impact risk event could be incidental and given a risk rating of 1.

Our members frequently find themselves in discussions with regulators over whether a third party is important enough to be deemed 'critical' rather than 'important' or 'ordinary.' The exact terminology changes depending upon the exchange/CCP or regulator but the conversations remain the same. While financial institutions' practices are designed to effectively manage the risks they face, a regulator may generally be more risk-averse than a financial institution.

We highlight this point to urge regulators not to seek to overapply the designation of 'critical.' Whilst the consultation tacitly acknowledges that risk assessments are conducted on a graduated scale, we are concerned that the

consultation could imply there is a simple binary distinction between critical and non-critical. Therefore, the finalised toolkit could benefit from a small section noting the graduated scale of risk management practices. Alternatively, sections 2.1 or 2.4 could be augmented to include this information.

Overall, we appreciate the FSB's intention to adopt a risk-based and flexible approach, as this allows individual financial institutions to develop and apply approaches to assessing their third parties that considers the degree of a given third-party's criticality, using, for example, rating scales.

6. Are there any tools that financial institutions could use in their onboarding and ongoing monitoring of service providers that have not been considered? Are there specific examples of useful practices that should be included in the toolkit?

The toolkit rightfully highlights that the nature and detail of contracts (or other similar arrangements) should be appropriate for the individual financial institution and criticality of the given service. In line with providing for appropriate contractual agreements, it is worthwhile to highlight that while asking services providers to take out insurance against certain risks may be a helpful tool, it is not always the appropriate risk mitigant as not all risks can be adequately insured against. For example, cyber-insurance coverage can be poor in certain cases. Policies can be expensive with high excesses/deductibles that ultimately, provide for insufficient coverage. Broadly, since insurance coverage may be challenging to acquire for certain risks, any requirement to have such insurance could create a barrier to entry for service providers. We hope that as the market continue to mature that these problems disappear. Nevertheless, this example is just to highlight that FIs would need to evaluate the costs/benefits trade-offs of employing any of the suggested tools.

Furthermore, along with the suggested commitments relating to resilience, it may be beneficial to note the possibility of including penalties for failing to meet commitments into third-party contracts. Penalties may be imposed under various scenarios, and they should be linked to what is "best in class" that is offered by vendors. Even if it is best in class, the penalty amount should not be so low that there is no consequence on vendors in cases where something goes wrong in order to incentivise the best provision of services.

Finally, the WFE disagrees with the proposal to identify key personnel involved in the delivery of the relevant service and their competency. It does not seem practical to start, keep and maintain a list of personnel identified in the delivery of a relevant service nor does it seem likely that third-parties would be willing or able to agree to contractual provisions requiring this. Instead, identifying contacts at the third-party should be sufficient.

7. What are the potential merits, challenges and practical feasibility of greater harmonisation of the data in financial institutions' registers of third-party service relationships?

As noted above, the WFE believes that financial institutions should continue to have flexibility to define their risk models based on the financial institution's use of a third party. Also noted above, a one-size-fits-all approach would likely not continue to provide that flexibility.

In addition, it will be challenging for firms to maintain certain information in real-time, and ad hoc requests should provide sufficient time for financial institutions to update their registers. Sharing of information with financial authorities should be risk-based, and the WFE does not believe that all new or proposed third-party relationships need to be disclosed, especially as there may be confidentiality clauses in Requests For Proposals.

8. Are the tools appropriate and proportionate to manage supply chain risks? Are there any other actionable, effective and proportionate tools based on best practices that financial institutions could leverage? Are there any other challenges not identified in the toolkit?

The toolkit appropriately intends to provide for a proportional approach that focuses on those nth-party service providers that are knowingly essential to the delivery of critical services or which have access to confidential or sensitive data, but there are limitations even in this regard with respect to financial institutions management of nth-parties' risks. WFE appreciates the FSB's recognition that there are challenges and limitations that supply chain risk management involves. It can be hard for each financial institution to directly assess and manage every individual risk across every component of their third-party service providers' supply chains because of the lengthening and increasing complexity of service providers' supply chains, especially in industries like Information and Communication Technology (ICT). Additionally, as it relates to nth-party service providers, contractual provisions may include confidentiality, whereby obtaining access to audit reports and test results may be difficult. In addition, being notified of nth degree provider outages may be challenging unless expressly provided in the contract.

Financial institutions' capacity to directly monitor and manage these risks has practical constraints. These are, as the consultation says, based on the costs, resourcing and time implications; gaps in information provided by third parties; and the limited ability for financial institutions to influence third parties, particularly large multinational companies. Financial institutions, particularly smaller ones, might struggle to meet the costs related to monitoring the supply chain, whereas larger financial institutions are likely to have longer and more complex supply chains that can be challenging to manage. Financial institutions are limited in their area of influence and may not be able persuade nth parties to report to them (eg, outages). Along these lines, while information on key supply chain dependencies and contractual provisions can be used to manage the risks from service providers' supply chains, as the toolkit references, one of the primary tools a financial institution relies upon is the practice of it validating that the third-party it faces directly has its own TPRM programme to adequately manage its service providers. This is the appropriate approach to take that is for financial institutions to use their TPRM and operational resilience programmes to manage risks across their service providers, which typically has a trickle-down effect, as opposed to attempting to manage 4th and nth-party providers.

For most financial institutions it will also simply not be practical to look far down the supply chain. Yet, the FSB proposal does not acknowledge this case and merely says that risk management should be applied in a proportionate manner. The distinction between key nth level parties and nth level parties is beneficial but it would, in fact, be proportionate to note that it is not always practical to look at nth parties, especially in terms of receiving timely notifications of planned changes to key nth-party service providers.

9. What do effective business continuity plans for critical services look like? Are there any best practices in the development and testing of these plans that could be included as tools? Are there any additional challenges or barriers not covered in the toolkit?

Business continuity plans must be tailored to the financial institution adopting them (eg, services provided) and consider the unique features of its relationship with third parties, such as the services the financial institution has determined to be critical to it that are provided by a given third party. Broadly, financial institutions must have the appropriate flexibility to continue to adopt and employ business continuity plans that are appropriate for their offerings.

It is important to recognise that there are certain challenges with respect to business continuity planning not considered by the consultation. The FSB uses the example of data and infrastructure provision in discussing business continuity planning which provides a helpful example to build upon:

"For instance, in the case of data and infrastructure, financial institutions may have options including but not limited to:

- *Using multiple data centres, whether from the same geographical region or spread across multiple regions;*

- *Combining on-premises and external (non-exclusive) data centres;*
- *Using multiple service providers, or a primary and back-up provider;*
- *Retaining the ability to bring data or applications back on-premises; or*
- *Any other viable options that can deliver a level of resilience consistent within the financial institution's risk appetite and tolerance for disruption."*

Using multiple data centres across multiple regions may work for some, but it also may present practical and regulatory barriers for others. For example, issues such as data protection regulations and sanctions may prevent the use of data centres in multiple jurisdictions and therefore, this approach may present other risks.

Combining on-premises and external data centres in a hybrid solution may also be overly complicated and costly. Bottlenecks can exist when moving data from one to the other, and the costs can rise quickly as the cloud solution will likely require different security measures, for example. Some WFE members are exploring or actively using hybrid models, but the ability to do so depends upon their individual circumstances. Using multiple service providers or a primary and back-up provider may also run into problems of interoperability. For example, data hosts do not operate interoperable systems, which means that there will be associated costs in developing a system that permits interoperability where that is deemed necessary by the individual financial institution.

Some services may not have ever been on-premises and therefore retaining the ability to bring them back on-premises may not likely be an appropriate option. For example, many newer or smaller exchanges may rely on third-party services to provide core services, including technologies like the order matching system. The ability to make use of third parties like these has resulted in growth in the number of exchanges, thereby introducing competition and fulfilling regulatory goals. An attempt to bring these services "back on-premises" may result in the exchange shutting down if it would not be able to meet the costs. This would be a poor outcome for less mature financial markets across the world.

Broadly, it is helpful to recognise that there are various practical, regulatory, and geo-political challenges with the application of business continuity plans.

Considering the specific recommendations noted in the toolkit, it will be difficult for financial institutions to receive detailed information related to vulnerabilities and remediation activities of service providers, and financial institutions themselves may not be willing to provide this information when they are third parties to others.

With regards to joint business continuity testing, the WFE would underline that current practices are adequate for risk management. This is currently accomplished via various sector work that has been going on for years and follows mature frameworks. Sharing information and programme maturity levels should be sufficient.

10. How can financial institutions effectively identify and manage concentration and related risks at the individual institution level? Are there any additional tools or effective practices that the toolkit could consider?

The WFE believes the consultation's approach of not proposing a singular and prescriptive manner for individual financial institutions to assess concentration risks is appropriate, recognizing that the criticality of a service varies across institutions. The consultation also appropriately highlights that while concentration is a risk, it can also bring synergies. For example, global cloud service providers can offer some of the most secure storage of data available because, in part, they benefit from economies of scale and excess profits can be re-directed towards technological innovation. Furthermore, as they are global, they can offer global reach, enabling businesses to fail-over into different jurisdictions. In addition, due to their ability to allow an FI to scale up and down quickly cloud service providers may

be more responsive in meeting sudden capacity needs (eg, when there are volume spikes) than on premises data centres.

11. Are there practical issues with financial institutions' third-party risk management that have not been fully considered?

One issue not considered is the potential conflicts of interest risk involved with third parties. Financial institutions serve customers which includes vendors. Exchanges take care to make sure that there are no conflicts of interest between those vendors that are listed on their own exchange and themselves.

Chapter 4

12. Is the concept of "systemic third-party dependencies" readily understood? Is the scope of this term appropriate or should it be amended?

With respect to the concept of "systemic third-party dependencies", a single financial institution, may not have sufficient information to gauge which vendors' failure and disruption may have financial stability implications. To the extent that a financial authority may have or gathers such information, WFE advises that they share it with relevant financial institutions so they can take financial stability implications into account when assessing third-party risks to their organizations.

WFE is concerned, however, about how an initial list of systemic third-party dependencies, once created, is maintained and remains current. Frequent ad hoc requests for information may place additional burdens on financial institutions that are not commensurate to the risks to their organizations.

13. How can proportionality be achieved with financial authorities' identification of systemic third-party dependencies?

14. Are there any thoughts on financial authorities' identification/designation of service providers as critical from a financial stability perspective?

The FSB defines systemic risk (with our emphasis added) as "a risk of disruption to financial services that is (i) caused by an impairment of all or parts of the financial system and (ii) has the *potential to have serious negative consequences for the real economy*. Fundamental to the definition is the notion of negative externalities from a disruption or failure in a financial institution, market or instrument." As we have seen in the recent past, financial instability is primarily a result of liquidity crises caused by insolvency of financial institutions. Operational disruption, while undesirable (and therefore subject to strenuous efforts to minimise) is a different matter.

Any regulatory policy in relation to third-party risks should be based on credible scenarios. Financial institutions invest huge sums to minimise operational risk. However, nothing they do can guarantee that there are no technical problems or that cyber-attacks will not occur, and this could be linked to the failure of a third-party. Nevertheless, market outages are subject to well established procedures at market infrastructure operators, and even the largest outages have not caused an exchange to go insolvent. We do recognise that it is prudent to prepare for eventualities. Our discussion is set out to provide context and underline the need for proportionality.

15. Should direct reporting of incidents by third-party service providers within systemic third-party dependencies to financial authorities be considered? If so, what potential forms could this reporting take?

We disagree with the proposal for service providers to provide direct access to their incident reporting platforms to the financial authorities, and for ad hoc requests, sufficient time should be provided for a financial institution to respond. Should financial authorities wish to receive information in a manner that is effective, secure, and ensures confidentiality, the WFE recommends that the financial authority establish a portal for all to use and report.

A more helpful tool for FIs would be for regulators to aggregate information from the regulated entities to see where there is sectoral concentration risk and provide this information back to the firms to incorporate into their third-party risk management programmes.

16. What are the challenges and barriers to effective cross-border cooperation and information sharing among financial authorities? How do these challenges impact financial institutions or service providers?

The challenges and barriers to effective cross-border co-operation and information sharing relate to differing regulatory requirements. Differing regulatory requirements can result in different reporting requirements. This makes it more difficult for regulators to share information across borders as they will principally rely on the information given to them by the regulated financial institution. That financial institution will present the information in different ways depending upon the supervisory expectations of different authorities. This also creates additional costs to the financial institution, as the financial institution has to create multiple reports. If a service provider is asked to provide information to fulfil regulatory requirements in multiple different jurisdictions, additional challenges may occur.

As noted above, the WFE believes that financial institutions should continue to have flexibility to define their risk models based on the financial institution's use of a third party. Any attempts to harmonise regulatory requirements or reporting requirements should not undermine this as this could weaken FIs ability to manage third-party risks. Instead, harmonisation should be undertaken on a principles-based approach that respects differing regulatory, supervisory and cultural approaches to third-party risk management.

Finally, the WFE would like to underline three concerns regarding cross-border information sharing, namely: (1) the potential for threat actors to obtain information; (2) relinquishing confidentiality, especially if there are confidentiality clauses in contracts; and (3) how substitutability will be maintained/updated, as it will change over time. Proposed changes should not place unnecessary burdens on the financial institutions involved.

17. Are there any views on (i) cross border information sharing among financial authorities on the areas covered in this toolkit (ii) including [certain third-party service providers] in cross-border resilience testing and exercises, including participation in pooled audits and?

It would be helpful if financial institutions could rely on cross-border resilience testing and exercises, to reduce duplication. Financial authorities should exercise caution in sharing financial institution's reviews of third-parties, as they may have different uses cases and due diligence requirements. Also, confidentiality clauses should be enforced.

18. Are there specific forms of cross-border cooperation that financial authorities should consider to address the challenges faced by financial institutions or service providers?

Further use of deference regimes, such as equivalence and mutual recognition, have proven to be beneficial across the financial industry and to the extent necessary, these regimes should also be embraced with respect to TPRM oversight. In particular, to prevent financial institutions and third parties from fulfilling multiple, possibly competing

requirements, deference regimes that determine other jurisdictions have sufficient controls in place on an outcomes-basis should be adopted by policy-makers.

Furthermore, the method being used to achieve greater convergence in cyber incident reporting could be a model for considering incident reporting elsewhere. The Format for Incident Reporting Exchange (FIRE) could be transformational in harmonising the format for reporting standards. However, burdensome requirements without the associated risk management benefits should be avoided, as it is unreasonable to expect financial institutions to report and notify financial authorities of every change, especially for sub-contractors.