8 January 2021

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

GFMA Consultation Response: Outsourcing and third-party relationships

The Global Financial Markets Association ("GFMA[1]") welcomes the opportunity to comment on the Financial Stability Board ("FSB") Discussion Paper (the "Discussion Paper") on *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships* published on 9 November 2020. The Discussion Paper provides an overview of the regulatory and supervisory landscape on outsourcing and third-party risk management in FSB Standing Committee on Supervisory and Regulatory Cooperation member jurisdictions, and seeks comments on four specific questions to facilitate discussions among authorities (including supervisory and resolution authorities), financial institutions and third parties.

Introduction to the GFMA

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

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

Please see below an executive summary of our members' responses, followed by detailed responses to the questions posed in the Discussion Paper.

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

---

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

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

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

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

Executive Summary

By way of overview, please see below a summary of the key matters raised in response to the questions posed in the Discussion Paper:

- As an overarching principle, we believe that regulations on third-party relationships should adopt a risk-based and outcome-focused approach that provides financial institutions with the ability to account for the different risk characteristics of various third-party relationships of different nature. Regulators should avoid imposing prescriptive obligations on financial institutions as this may compromise the efficiency and resilience of financial institutions and create discrepancies between regulations across jurisdictions.

- Global consistency on scope and definitions of commonly used key terms including the terms "outsourcing" and "third-party relationships" is required, enabling financial institutions to obtain a clear and consistent view of risk across jurisdictions.

- More specifically, in relation to the taxonomy of key terms, we identify a need to differentiate between third party-services of different nature (e.g. financial services regulated service providers, financial market utilities, non-financial services regulated entities, entities within the same group, third parties providing critical services) as both financial institution and supervisory oversight should be proportionate to risks.

- Global consistency of standards and treatment across jurisdictions is also required. Different jurisdictions have varying degrees of prescription with respect to regulatory approaches, including in relation to cloud outsourcing, regulatory reporting of outsourcing inventories, approvals, data access and data localisation policies, and the standards applied to assess the criticality of certain outsourcing transactions or third-party relationships. Fragmented and prescriptive regulatory regimes that impact global financial institutions' outsourcing and third-party relationships represent a fundamental challenge for the efficient management and mitigation of risks.

- From a practical perspective, we see the need to coordinate the timing of consultation and release of new regulations across jurisdictions in order to enable financial institutions to adapt to regulatory changes with sufficient time and in a globally coherent way. Our members stress the importance of maintaining their focus on managing risks but have indicated that it becomes difficult to do so if new consultations and rules are persistently being issued in the various jurisdictions in which they operate.

- In respect of cloud technology, a key concern of our members is that if the use of cloud as part of an outsourcing arrangement and third-party services would become an automatic indication of risk, leading to an imposition of the same set of regulatory standards, without an appropriate assessment of key risk attributes such as service, scope and infrastructure of the cloud arrangement.

- Supervisors should take a proportionate approach to intra-group outsourcing compliance, proving local entities with the ability to rely on well-controlled and globally consistent group policies and processes. Furthermore, intra-group outsourcing provides for effective operational resilience and risk management for financial institutions. Supervisors should therefore seek to adopt a risk-based approach and avoid the replication of the provision of systems, data or processes within local entities which itself increases operational risk and complicates firms' resilience strategies.

- Further, we caution against the implementation of data localisation measures which can also result in the need for financial institutions to replicate the provision of systems, data or processes within a local entity, ultimately contributing to operational risk. In lieu of data localisation policies, our members are of the view that regulators should consider establishing information sharing regimes to address the concern that regulators require the ability to access information relating to services performed by third-party service providers outside the jurisdiction.

- In respect of the potential systemic risks arising from the concentration of third-party services, it is important to differentiate between the concentration risks that may exist where

multiple regulated entities use a common service provider (sector-wide concentration risks) and instances where a group is dependent on a single service provider for the provision of outsourced tasks (internal dependency). In relation to financial sector-wide systemic risks, we are of the view that financial regulators are better-positioned to assess such risks at an industry level, rather than financial institutions individually but financial regulators should leave it up to the financial institutions to mitigate the risks associated with that concentration. However, members recognise that concentration risks are unlikely to be fully mitigated by regulation and consider that global and national financial authorities should work closer together to explore how the risk of major operational incidents suffered by key service providers which may impact financial stability could be better addressed. We caution against the imposition of prescriptive obligations on financial institutions in order to mitigate concentration risks, and we maintain that financial institutions should have the freedom to select their third-party service providers and not be mandated by regulations to exit or duplicate their outsourcing arrangements or third-party services. In the case of concentration risks that arise from a group depending on a single service provider, we believe that firms should be able to undertake an internal assessment based on risk appetite, and not be mandated to assess concentration risk arising from its outsourcing and third-party relationships on stipulated metrics that are set in regulatory guidance. Such an approach could affect the ability of a regulated entity to manage its oversight obligations and continuously enhance its resilience capabilities. Individual firms can and should be able to practice their incident and risk management in this area.

- We acknowledge that there are practical challenges in terms of contract negotiation and actual implementation of audits and due diligence requirements with certain third-party service providers (including, the assessment of third-party service providers' operational resilience measures). Further, the ability of financial institutions and regulators to control risks relating to the management of sub-contractors where there is a long supply chain is limited. We suggest that the use of pooled audits, third-party certifications and shared assessments may assist in enhancing the efficiency of due diligence down the value chain.

- We support further input to global discussions on the direct oversight by regulators of critical third parties. We consider direct oversight may be one possible approach for addressing concentration risk.

- As financial services are a global and interconnected sector, we support further cross-border collaboration between regulators, financial institutions and service providers, to limit the risk of inconsistent regulatory requirements. We identify that areas that would benefit from such cross-border collaboration, including in the assessment of concentration risks, rehearsals of disruptive events in the market, how to best realise regulators' ability to access data for supervision purposes and general regulatory alignment and coordination. To facilitate such cross-border collaboration, we also suggest establishing channels for collaboration, such as public-private forums, public consultations, global supervisory colleges and information sharing and collaboration platforms.

- Last but not least, in response to the FSB's last question in the Discussion Paper, we wish to highlight our members' feedback on the lessons learned from the COVID-19 pandemic in the past year, which we believe has significance on the future development of the regulatory landscape. As a high-level summary, we believe that the pandemic demonstrates the importance for financial institutions to adopt a risk-based approach and focus on operational resilience in managing outsourcing and third-party risk exposures. We see a need to plan for longer term recovery in addition to addressing short-term impact events (e.g. service level agreement ("SLA") deterioration) and consider that the performance of control functions need to be more dynamic to cope with exceptional circumstances. Over the course of the pandemic, our members have developed a greater reliance on technology. In terms of managing operational resilience, cloud technology has emerged as an important risk management tool, and therefore, consultations encompassing the appropriate regulatory oversight for cloud providers has an increased significance for our members.

Thanks again for providing us with the opportunity to comment on the Discussion Paper. We and our members stand ready to engage on this topic further with FSB. We look forward to having the opportunity to provide further assistance as regulations governing outsourcing and third-party relationships continue to be refined.

Respectfully,

Allison Parent
Executive Director
Global Financial Markets Association
www.gfma.org

Consultation Response

Q1. 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?

Q2. 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?

We set out below our members' responses to Questions 1 and 2 of the Discussion Paper. Each section highlights an area of challenge relating to outsourcing transactions and third-party relationships and proposes mitigation strategies to such challenges. In summary, the key areas which have been identified include:

- **outcomes and risk-based approach** - supervisors are encouraged to adopt proportionate, risk-based and outcomes-focused approaches to third-party arrangements;
- **regulatory scope and definitions** – global consistency on regulatory scope and definitions is required;
- **regulatory fragmentation** – alignment of disparate regulatory requirements and coordination of the timing of consultation and release of new regulations across jurisdictions are required;
- **regulation of cloud service** – a risk-based approach should be adopted and any regulation should be able to keep pace with technological advancement;
- **intra-group outsourcing** – intra-group outsourcing on a cross-border basis can reduce overall risk while improving efficiency. Supervisors should not prevent or hinder intra-group outsourcing, should treat it differently than external outsourcing, adopt a risk-based approach in the context of intra-group and inter-branch transactions and avoid the replication of the provision of systems, data or processes within local entities which itself increases operational risk and complicates firms' resilience strategies.
- **data localisation restrictions** –data localisation restrictions contribute to operational risk and a home-to-host information sharing regime may be sufficient to address the risks which local regulators seeks to address under an overseas outsourcing arrangement/third-party service;
- **risk of concentration of third parties** – financial regulators should work with financial institutions and third parties to gain visibility into the risks that arise from systemic concentration risks rather than the concentration itself;
- **supply chain management** – use of efficiency-enhancing methods such as pooled audits, third-party certifications and shared assessments may assist in overcoming the practical challenges of overseeing third parties and managing supply chains; and
- **direct oversight of critical service providers** – further discussion on a global level is required.

A. OVERARCHING PRINCIPLES: REGULATIONS TO ADOPT A RISK-BASED, OUTCOME-FOCUSED AND PRINCIPLES-BASED APPROACH

As an overarching principle, we emphasise that regulators and standard setters should adopt a risk-based and outcome-focused approach to formulate and implement regulations and

guidelines that are proportionate to the risk characteristics of different third-party relationships. In the case of regulated service providers, such as financial market infrastructures ("FMIs")[5], the risk assessment should take into account the fact that FMIs are regulated and single source (and not automatically deemed high-risk solely because FMIs support large dollar payment processes). Accordingly, it is important that there is clarity on how various third-party relationships are defined and differentiated under regulatory frameworks. This will be further discussed in detail in section B.

Additionally, we stress that regulators should avoid imposing prescriptive obligations on financial institutions. Prescriptive regulations, such as requiring the use of local service providers only, requiring the adoption of multi-vendor solutions (i.e. to replicate services across more than one provider), imposing quotas per vendor and mandating financial institutions to assess sector-wide concentration risks, may compromise the efficiency and resilience of financial institutions by limiting financial institutions from enhancing their own resilience capabilities and to adapt to emerging business models and technologies Excessive regulatory controls can stifle innovation or accentuate concentration or ICT risks and increase operational costs by raising barriers to entry.

Further, prescriptive approaches from various regulators may have potentially unintended consequences, including, discrepancies in the definitions of key terminologies, assessment of materiality and reporting requirements. This in turn will create a fragmented picture of risks and ultimately inhibit global financial institutions from obtaining a clear view of their key risks (such as concentration risks) across jurisdictions where they and service providers operate.

On an additional note, while regulators and standard setters should ensure regulations and guidelines are not prescriptive, to the extent that procedural requirements (e.g. reporting or governance process) are mandated, we urge regulators to ensure that such procedures are set out clearly to avoid ambiguity.

B. REGULATORY SCOPE AND DEFINITIONS

Disparate Regulatory Scope and Definitions

The first key challenge in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, is understanding the inconsistent and often convoluted references to "outsourcing" and "third-party relationships" and "materiality/criticality" across different jurisdictions and regulators, as both terms are broadly defined, and may be interpreted differently under different regulations and guidelines.

We note that some regulators are gradually moving away from the definition of "outsourcing" towards a more holistic notion of "third-party relationships". It is noted that the Discussion Paper seeks to encompass both "outsourcing" arrangements and "third-party relationships". As a convenient reference, the Discussion Paper has noted the example of the Basel Committee on Banking Supervision's ("BCBS") August 2020 consultative document on Principles for operational resilience, which apply to "all dependencies on a bank's relationship with third parties or intra-group entities relevant to the delivery of critical operations".

We acknowledge that this shift in approach may move away from a prescriptive approach which requires extensive analysis to ascertain whether an arrangement is, or is not, in scope of outsourcing regulation. However, we emphasise that in any framework that moves towards a holistic notion of "third-party relationships", it is important to adopt the risk-based and outcome-focused approach. A deviation from such approach, such as imposing uniformly stringent requirements across all types of "third-party relationships", will broaden the regulatory scope both qualitatively and quantitatively. Consequentially, such unnecessarily broadened scope will divert attention away from arrangements that pose the most risks, significantly impact existing review pipelines and capacities of financial institutions, and lead to even more challenging vendor contract negotiations (as well as challenges in the management of existing vendor contracts).

[5] Financial market infrastructures (FMI) is a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

Clarify Regulatory Scope and Definitions

Regulating Different Third-party Relationships

As a starting point, we stress that entities within the same corporate group of a financial institution should not be treated the same as other external third parties. Regulators should take into account the principle of proportionality in terms compliance with outsourcing rules, as such entities are often subject to well-controlled and globally consistent policies and processes. . We note that the regulatory approaches on how intra-group entities are treated have not been entirely consistent. In particular, we note the inconsistent approaches between the draft PRA Supervisory Statement (the subject of the PRA consultation on Outsourcing and Third-Party Risk Management[6]) which are intended to apply to transactions between branches of the same entity, and the EBA outsourcing guidelines, which do not apply to transactions between branches as such arrangements are not considered to be outsourcing. Likewise, financial institutions' relationships with regulated third parties and FMIs which are well-known and already regulated should be subject to different regulatory treatment (such as the degree of oversight required) proportionate to the risks involved. Moreover, the failure to distinguish regulated entities from other third-party providers may result in a duplication of regulatory regimes. For example, the recent PRA consultation on Outsourcing and Third-Party Risk Management proposed financial institutions to "assume that activities, functions, services performed or provided by third parties in a 'prudential context' … fall within the definition of 'outsourcing'". As such, this approach could arguably bring into scope activities such as custody services, depositary services, clearing/settlement services, collateral management services and other activities performed by financial intermediaries which are already regulated through multiple rules and requirements, creating a more complex regulatory landscape.

Definition of Outsourcing

In relation to the definition of "outsourcing", where regulatory standards distinguish "purchasing contracts" from the concept of "outsourcing" (e.g. as proposed under IOSCO's Consultation Report on the Principles on Outsourcing[7]), some members consider it difficult to categorise whether an arrangement constitutes "outsourcing" or "purchasing contract". By way of example, financial institutions often rely on third parties for managed services of computer equipment or infrastructure that is owned by the regulated entity. However, the third-party personnel engaged in the provision of the managed services may not necessarily have logical access to the non-public proprietary or client information stored on the equipment. Arguably this is a service that the regulated entity would otherwise undertake itself. In this situation, it is unclear whether such a procurement would constitute an "outsourcing" or merely a "purchasing contract". In light of the above, where regulatory standards take into account the concept of "purchasing" in determining whether an arrangement constitutes "outsourcing", we consider there is a need for additional guidance and (if possible) supplementary illustrative scenarios and parameters to assist financial institutions in further distinguishing between "outsourcing" and "purchasing" transactions.

Another example scenario is "partnerships with third parties" (e.g. partnerships with FinTech companies). Such partnerships often involve the consumption of services provided by business partners as part of an overall strategic partnership transaction, but it is not clear to some of our members whether such arrangements could fall within the scope of "outsourcing". This illustrates the need to align and clarify the definition of "outsourcing" in order to ensure that consistent measures are adopted across various financial institutions as a whole.

In light of the above, we urge regulators to take a consistent approach to regulatory scope to allow financial institutions to be able to differentiate "third-party relationships" of different nature from each other, and implement suitable risk management measures that are proportionate to the risks involved and align to other regulatory frameworks such as recovery and resolution and operational resilience. Specifically, for IT outsourcing, certain members express the view that the emphasis of regulation ought to focus more on public IaaS

[6] PRA (2019) *Outsourcing and third party risk management*, December 2019.

[7] IOSCO (2020) *Principles on Outsourcing Consultation Report*, May 2020.

commercial providers given they provide distinct technical IT services and underpin other types of IT outsourcing (PaaS and SaaS).

Furthermore, to allow financial institutions to effectively manage third-party risks in accordance with regulatory guidelines, there is a need to clarify and reconcile the existing different definitions of the key terms including "outsourcing" and "third-party relationships".

We believe that the FSB, as an international body for monitoring and making recommendations about the global financial system, can lead the coordination of regulators and standard setters to determine a set of consistent definitions for the key terms related to outsourcing and third-party relationships.

C. REGULATORY REQUIREMENTS AND IMPLEMENTATION SCHEDULE

Disparate Regulatory Requirements

The fragmented regulatory regimes that impact global financial institutions' outsourcing and third-party relationships is a fundamental challenge for the efficient management and mitigation of risks. Our members expressed that the onerous requirements to comply with very specific and nuanced local requirements can be resource-intensive and a distraction to their fundamental management of risks.

We set out below some examples of regulatory requirements or approaches that we identify to be inconsistent and would benefit from regulatory alignment:

- **Definition of Outsourcing and Third-Party Relationships:** Despite supervisory authorities having broadly leveraged the definition of "outsourcing" in the 2005 Joint Forum report on Outsourcing in Financial Services, as noted above, there remains uncertainty in relation to how to apply the definition of outsourcing. Additionally, there continues to be differences across the globe on scoping "third-party relationships" and the interpretation of other key terminologies.

- **Criticality:** The standards of criticality across different jurisdictions are inconsistent and remain one of the challenges in complying with regulatory requirements. In particular, regulations and guidelines have promulgated standards such as "critical and important function" or "materiality". It is worth noting that financial institutions need to also assess external outsourcing arrangements and third-party services in light of terms such as "important business services" and "critical operations" in the context of operational resilience.

- **Cloud:** Regulators diverge on approaches to oversight of cloud service providers driven by views of innovation risk, national sovereignty, competition and systemic risk, all of which contributes to global financial institutions having to manage their cloud service providers in a fragmented way, to address such jurisdictional differences. Furthermore, there also appears to be an element of conflicting regulatory trade-offs, with financial institutions being asked to consider data storage optimisation that is not solely-dependent on physical or hardware solutions, yet to proceed with caution and comprehensively assess the risks associated with an external cloud or outsourcing provider. Our members have noted that it is difficult for financial institutions to utilise the advantages of cloud technology and similar technological innovations without relying on external third-party providers.

- **Data Access:** Certain outsourcing regulations require financial institutions to obtain confirmation from a foreign regulator to ensure the ability of the local regulator to have continued access to information relating to an outsourcing arrangement, where that service is provided outside the financial institution's jurisdiction.[8] This presents a challenge that is outside the control of financial institutions, and may lead to a fragmented delivery model for financial institutions where services can only be provided in-country and result in a need to replicate the provision of systems, data or processes

[8] MAS (2019) *Response to Feedback Received - Outsourcing by Banks and Merchant Banks*, November 2019, paragraph 10.4.

within a local entity, as opposed to relying on group-wide global systems, data or processes through intra-group outsourcing.

- **Data Localisation:** Data localisation policies of some regulatory authorities require outsourced data to remain in the same jurisdiction as the relevant financial institution. These policies may limit the potential enhancements to financial institutions' operational resilience using third-party tools such as cloud services or intragroup data storage facilities. Further, the fragmentation of data localisation policies across jurisdictions leads to the diversion of resources that are required to ensure organisations' data transfer and storing policies are compliant with the laws and regulations of every single country data is collected from.

- **Regulatory reporting of outsourcing inventories:** There are significant differences in the outsourcing registry/inventory requirements across jurisdictions. As such, the data required for the purposes of reporting on outsourcing transactions and third-party relationships is different across jurisdictions, which can inhibit financial institutions, and regulators, from obtaining a clear and consistent view of arrangements across jurisdictions.

- **Approvals:** There are instances where lengthy regulatory approval periods are required for material outsourcing arrangements, and information to be provided as part of the approval process differs across jurisdictions, which affect financial institutions that may rely on those arrangements for business continuity or resilience purposes. To the extent that financial institutions need to quickly respond to the changing operational environment by relying on outsourcing arrangements, lengthy approval periods may disrupt the ability to ensure the seamless provision of services.

Lack of Coordination in Implementing Regulatory Standards

We are also concerned that there is a lack of coordination among regulators and standard setters in terms of the consultation and implementation timetables for regulations. There have been multiple instances in which different regulators have implemented new regulations in respect of the same or similar regulatory scope, leading to ambiguity among global financial institutions. Further, regulators across jurisdictions have been at a rush to introduce new regulations and policies concerning information technology. The everchanging regulatory landscape and influx of new rules exacerbates the fragmentation of regulatory approaches and make it difficult for financial institutions to keep pace with the implementation timeline across their global offices and significantly increases the costs of compliance and the rate of change to be implemented. A high rate of regulatory change can prevent institutions' from obtaining a clear and coherent view of risk when the regulatory environment is constantly changing.

Regulatory Alignment and Coordination

We believe that regulatory alignment is important to avoid fragmentation of the regulatory landscape.

First, we encourage regulators to rely on existing policies and processes wherever possible to address outsourcing/third-party relationship risks rather than the introduction of additionally policies or processes, which will complicate the regulatory landscape.

We also urge regulators to collaborate to develop consistent regulatory approaches that apply across jurisdictions and interconnected regulatory policy topics and are interoperable globally. Global collaboration would allow for better sharing of information and lessons-learned. We will further discuss our suggestions on global collaboration efforts and channels in our response to Question 3.

Further, our members support the use of international certifications to form part of the solution to align regulatory standards across jurisdictions. For instance, international regulators and standard setters may together recognise certain certifications and standards (e.g. those of the International Organisation for Standardization (ISO)/International Electrotechnical Commission (IEC), SOC 2, NIST Cybersecurity Framework and the CPMI-

IOSCO Guidance, Financial Services Sector Cybersecurity Profile (FSP)[9], etc.) as benchmarks for compliance. Applying a consistent standard across jurisdictions and between regulators will allow the risk management process of financial institutions to be more efficient and effective.

Practically, cross-jurisdiction coordination of regulatory consultations is essential to enable financial institutions to adapt to regulatory changes in a timely manner, allowing financial institutions to maintain their focus on managing risks whilst ensuring compliance with new regulations.

We believe that FSB could play the coordinating role in such international engagement to harmonise regulatory approaches, align intended outcomes and timing of consultations, as well as implementation of regulations and policies.

D. REGULATION OF CLOUD SERVICE

As identified in the Discussion Paper, there is an increasing trend of cloud services-specific regulations, which the BCBS describes as an "enabling technology" that provides the underlying infrastructure for many FinTech activities and other technology solutions[10] utilised by the financial services industry.

We are concerned that the use of cloud technology as part of an outsourcing arrangement will become an automatic indication of risk, leading to an imposition of the same set of regulatory standards without an appropriate assessment of key risk attributes such as service, scope and infrastructure of the cloud service arrangement. For example, a private cloud that is wholly owned and managed within a corporate group for exclusive use by the single corporate group is much more akin to traditional on-premises models of IT provision, where inter-affiliate service is well established, than some other uses of (public) cloud. Under such private cloud arrangements, the financial institution's legal entities would have enhanced oversight of, and input into the design of, the mitigating controls put in place. However, we believe firms should also be able to reference the established inter-affiliate service model as part of their governance framework for private cloud. Such outsourcing engagements (e.g. engagements that are supported by applications/systems that are hosted on a private cloud or data that is processed via a private cloud) should not be automatically perceived as more susceptible to risk than that provisioned through traditional shared technology/hardware models. Rather, each cloud arrangement should be subject to an assessment for identifying the particular risks involved.

In addition, we note that data segregation can often be a requirement under outsourcing regulations and guidelines. This can present challenges in the context of cloud outsourcing given data are generally stored in a shared environment. In particular, it is noted that physical segregation of data is not generally possible, but that logical segregation may be feasible.

Adopt a Risk-based Approach in Regulation and Keep Pace with Technology Advancement

Given the benefits to using cloud technology (including as recently noted by IOSCO),[11] if all cloud models were to be treated in the same way and subject to heightened regulations, such regulations may stifle the ability to realise the benefits of cloud technology, while not being commensurate with the relevant risks.

On an additional note, we wish to point out that we are currently in a transitory period in relation to technology provision. We expect that in the foreseeable future, cloud technology will become the norm.. Any regulatory development will need to keep pace with the trend to ensure that the financial sector can take advantage of technology efficiently to maintain a competitive edge and leverage the risk and resiliency benefits that cloud provides, as compared to the maintenance of legacy infrastructure.

---

[9] Cyber Risk Institute (2020) *Financial Services Sector Cybersecurity Profile*, November 2020

[10] BCBS (2018), *Sound Practices: implications of fintech developments for banks and bank supervisors*, 19 February.

[11] IOSCO (2020), *Principles on Outsourcing Consultation Report*, May 2020.

E. INTRAGROUP OUTSOURCING

Members have noted that certain regulatory requirements may prevent or hinder intra-group outsourcing arrangements between geographies, even if this would be not only more efficient, but also more effective at achieving operational resilience and risk management for the financial institution than fragmented operations. As an example, through operating cyber defence capabilities on a global, firm-wide basis, our members can have cybersecurity centres in several global locations, providing 24/7 firm-wide coverage. This facilitates better cybersecurity capabilities and protection for our members' clients and for their local operations. If entities are only able to make use of cyber operations from their own jurisdiction, this would increase risk to local entities (noting that adversaries operate on a cross-border basis). Network defence cannot have national boundaries and the imposition of national boundaries will leave members exposed.

Supervisors should not prevent or hinder intra-group outsourcing, should treat it differently than external outsourcing, adopt a risk-based approach in the context of intra-group and inter-branch transactions and avoid the replication of the provision of systems, data or processes within local entities which itself increases operational risk and complicates firms' resilience strategies.

F. DATA LOCALISATION

We also note that some jurisdictions have or have proposed measures that require financial services and cloud service providers to store and process their data locally, including requiring "mirroring" of data on local servers or measures that prevent cross-border data transfers.[12] These supervisory practices may result in the need for financial institutions to replicate the provision of systems, data or processes within a local entity, as opposed to the safe, secure and appropriate reliance on global group-wide systems, data or processes.

Home-to-host Information Sharing

In order to combat the potential for regulators to require localisation of systems, data and processes provided by entities within a corporate group, we encourage the FSB Standing Committee on Supervisory and Regulatory Cooperation to establish an information sharing forum to facilitate home-to-host information sharing. This may assist in addressing some of the risks perceived by local regulators in relation to the exercise of their supervisory function and their ability to obtain necessary information on the outsourced or third-party service.

G. RISK OF CONCENTRATION OF THIRD PARTIES

The Discussion Paper raises the concern of potential systemic risks arising from concentration in the provision of some outsourced and third-party services to financial institutions.

First, we would like to highlight that concentration of third-party services is not per se undesirable, but the actual risks arising from such concentration should be assessed and addressed.

Second, in considering risks, it is important to differentiate between the concentration risks that may exist where multiple regulated entities use a common service provider (sector-wide concentration risks) and instances where a group is dependent on a single service provider for the provision of outsourced tasks (internal dependency).

Multi-vendor Strategies

We are of the view that recently emerging regulatory standards (e.g. the EU's proposed Digital Operational Resilience Act (DORA)[13]) that lean towards forcing a multi-vendor strategy on financial institutions could increase operational risks and challenge the global

[12] FSB (2019) *Third-party dependencies in cloud services: Considerations on financial stability implications*, 9 December.

[13] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. Can be accessed at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1

operating models of cross-border financial institutions. For instance, if financial institutions are required to bring outsourced services back "in-house" as a result of these measures, they will be effectively required to build out on-premise infrastructure and/or software (e.g. code libraries). As technology services are proprietary to the external party, financial institutions will not be able to bring "in-house" such proprietary services without significantly altering their application and/or interface with on-premise applications. Further, these rules may also be anti-competitive in practice (e.g. how would the regulators determine which financial institutions could use a particular provider). As such, we recommend that such measures should not be mandated, and the use of multi-vendor strategies should remain a risk-based and business decision of financial institutions.

Solutions in Relation to Regulating the Management of Concentration Risks

Sector-wide Concentration Risks

We believe that the right path forward in relation to all concentration risks, is not to seek the elimination, drastic reduction, or even equitable distribution of the risks; instead, the focus should be on gaining visibility into these risks, ensuring the right security and resiliency frameworks are implemented to manage these risks and working together deliberately and incrementally to create an environment which does not stifle the ability to utilise third parties.

In respect of regulation for oversight of concentration risks, we emphasise again the overarching principle that any regulatory framework should be risk-based. In other words, it is important that the regulatory focus of financial regulators is set on managing risks arising from concentration, rather than reducing concentration itself. Specifically, we consider that financial regulators should differentiate third parties of different nature when assessing the actual risk stemming from market concentration. For instance, FMIs are different from cloud service providers, as the former were built in the system for market efficiencies, and are known and regulated.

We urge financial regulators to avoid prescriptive obligations such as use of local service providers only, enforce multi-vendor solutions and quotas per vendor or mandating financial institutions to assess sector-wide concentration risks. In relation to the assessment of sector-wide systemic risks, we are of the view that supervisory authorities are better-positioned to assess such risks at an industry level, rather than financial institutions individually.

Any assessment of concentration risk by financial regulators should not restrict the choice of outsourcing arrangements or providers available to financial institutions. More fragmentation and complexity in financial institutions' operations are likely to make risk management more difficult and localised, resulting in greater aggregate risk at the global level.

We also ask financial regulators to closely consult with financial institutions in introducing any measures to address concentration risks. Industry and policymaker collaboration to support sector-wide resiliency is important to help identify potential risks and gaps across business services, given sector-wide interdependencies and substitutability across firms. Authorities both at the national level but also within the international standard setting bodies such as the FSB, should consider exercising their convening power to bring the industry and potentially relevant third parties together to begin exploring how major operational incidents that could impact financial stability would be addressed. While exercises and the development of play books will take time, and are unlikely to be sufficient to fully address risks arising from concentration, they are a necessary first step to making progress on this question.

Internal Dependency Risks

- In the case of internal dependency, we believe that financial institutions should be able to undertake internal assessments based on their risk appetite, and not be mandated to use stipulated metrics that are set in regulatory guidance (which may not be commensurate with the applicable risks) in order to assess the concentration of outsourcing and third-party relationships within the institution. Our members have, for instance, seen concentration measured as a percent of spend, which we do not believe accurately reflects risk. Such an approach could affect the ability of a regulated entity to manage its oversight obligations, continuously enhance its resilience capabilities, adapt to emerging business models and

technologies and make commercial decisions. Financial institutions are particularly concerned of regulatory measures which mandate the use of multiple service providers (to the detriment of other commercial/operational considerations) in circumstances where regulated entities are able to manage the concentration risk which arises from use of the same service provider. Intra-group outsourcing which is common among financial institutions (e.g. outsourcing a particular service entirely to an affiliate or head office), should be outside of the scope of assessing a firm's concentration risk. If processes are not allowed to spread across safe, reliable group-wide systems, this may result in undue replication of policies, processes or technology, with adverse impacts on risk (see our discussion about intragroup outsourcing under Questions 1 and 2).

Exit Plans

First, we emphasise that we do not agree with any regulations requiring financial institutions to exit a given third-party arrangement to address concentration risk and require financial institutions move the relevant function, service or data to an alternative service provider, back in-house or seek alternative methods to ensure the continued provision of the service.

Second, any resilience plans to recover and withstand from an outage should be treated differently from other failures of a third party. While exit plans including portability of the service are appropriate to consider in the event of a breakdown in the vendor relationship or total failure of the provider, we caution that they should not be considered to be appropriate contingency plans in the event of a service provider outage. Any attempt to migrate services or data during an IT incident could result in further operational risks and, in numerous instances, may not be possible given the proprietary nature of the service implementation of the external party. In the event that a service provider works with multiple regulated entities, regulatory requirements that result in the mass migration of services away from that service provider could destabilise the market and raise questions about the capacity of alternative providers and the potential for cascading outages. Existing regulations generally already require regulated entities to ensure the continued provision of the outsourced services and continued access to data. Our view is that the transfer of service is feasible in the event of a medium to long term migration away from a service provider in a controlled and planned manner but is not appropriate to address business continuity risk in the event of an IT incident.

H. SUPPLY CHAIN MANAGEMENT

Practical Challenges to End-to-end Oversight for Third Parties

Some members encounter practical challenges in terms of contract negotiation and actual implementation of audits and due diligence on third parties even when these form part of contractual obligations.

As accurately identified in the Discussion Paper, there may be an imbalance of negotiation power between financial institutions (depending on the size of the financial institution) and third parties (especially with prominent service providers), which affects the ability of financial institutions to ascertain certain pre-requirements and exercise effective oversight. In many instances, regulations place the obligation on financial institutions to effectively educate third parties of the relevant regulations and convince third parties that compliance with such requirements are a necessity. This can, at times, be particularly difficult with prominent service providers. It may be useful for regulators to publish guidance to the third-party service provider community on what they need to do when dealing with financial institutions or other institution types in the context of outsourcing arrangements and third-party relationships.

Moreover, in assessing the standard of operational resilience of third parties, the traditional methods for overseeing third parties' risk management system, such as conducting due diligence through questionnaires, interviews/meetings, and contractual clauses, may be incomplete as the process reviews the governance and preventative controls of the third party but does not measure whether the third party can restore operations within a specific timeframe. Therefore, the resulting outcome of a public/private effort on oversight expectations for resilience is important to inform this Discussion Paper.

Further, the regulatory requirement to conduct audits for each and every third party to the same level of diligence irrespective of the level of risks is unnecessary and against the principle of adopting a risk-based regulatory approach.

Limitations in Supply Chain Management

There are limitations in the abilities of financial institutions and regulatory authorities to identify and mitigate risks relating to the management of sub-contractors where there is a lengthy supply chain ("nth parties"), particularly at the 5th party level onwards.

Whilst financial institutions generally seek to hold their service providers accountable in relation to the service providers' subcontractors, they may have limited ability to contractually bind a subcontractor engaged by the financial institution's third-party service provider. Accordingly, it is also difficult for the financial institution to directly assess the operational resilience of that subcontractor and ensuring parity of safeguarding measures.

It should be noted that where financial institutions seek to manage the nth parties through the third-party service providers, in respect of due diligence, some third-party service providers can be reluctant to disclose contractual details and how they conduct due diligence of their sub-contractors (and even less third-party service providers are willing to provide the right for financial institutions to directly conduct due diligence in respect of their sub-contractors).

There are also challenges with the ability to impact sub-contracting arrangements that are already in place with a specific provider at the time of engagement with financial institutions. Third-party service providers can therefore be reluctant to amend those existing contracts in line with requirements of financial institutions. These challenges are exacerbated if financial institutions seek to impose obligations further down the supply chain with the nth parties.

Generalised expectations for direct oversight by financial institutions of nth parties must be avoided. Regulatory standards must acknowledge that for the majority of nth party relationships, the most practical and effective approach to managing risk is through the risk management processes with the primary service provider. New and growing emphasis requiring direct oversight of subcontractors leads to an exponential increase in assessments for financial institutions and providers in the supply chain, as well as the global market overall, substantially increasing the costs of compliance.

Pooled audits, Third-party Certifications and Shared Assessments

Our members are of the view that any regulatory or supervisory expectations for financial institutions related to supply chain management should be realistic and proportionate to the risks involved. For instance, the focus should be on critical outsourced providers (i.e. where the portion subcontracted is critical), and to obtain assurance that they have robust third-party risk and supply chain frameworks.

In regard to the practical challenges faced by financial institutions in auditing third-party service providers, we support the use of pooled audits and third-party certifications (e.g. ISO/IEC, SOC 2, NIST Cybersecurity Framework, Financial Services Sector Cybersecurity Profile (FSP) and the CPMI-IOSCO Guidance, Know Your Third Party (KY3P), etc.) as methods to make the exercise of access, audit and information rights more effective and efficient. One additional suggestion is the sharing and reuse of audit reports by other financial institutions in a utility-style model (provided that confidentiality is properly addressed and the subject and quality of the audit reports being compatible with the relevant auditing purposes). We understand that this is a complex area, as there may be issues relating to proprietary restriction on what may be audited, as well as corporate data associated with shared reports, and implementation of measures will require careful consideration and planning. Additionally, auditing in the case of cloud services is not traditionally "unrestricted" and is constrained to the scope set out in the relevant contract. The industry may require additional guidance on the regulators' expected level of assurance to be provided by audits and certifications. Shared assessments, or a utility-style model, would also benefit service providers who would be faced with fewer information requests.

In respect of third-party certifications, we acknowledge that they only form part of a holistic solution to address risks, but undue reliance without further scrutiny will be insufficient to provide the necessary assurance. Notably, the efficiency-enhancing methods suggested above do not alleviate financial institutions from their responsibilities to audit numerous third parties. Financial institutions are still required to allocate resources and expertise to review the audit reports and/or information in relation to the relevant certificates. Nonetheless, such reviews should be based on the risk of the external party relationship.

I. FURTHER DISCUSSION ABOUT DIRECT OVERSIGHT OF CRITICAL SERVICE PROVIDERS

Finally, our members would like to take this opportunity to address the widely-discussed suggestion of directly regulating critical third parties to mitigate risks in connection with outsourcing and third-party relationships.

We support further input to any global discussions regarding such direct oversight. Identifying, and supervising, at the global level third-party service providers which provide "critical" services and/or represent a concentration of services across the sector, is one possible approach for addressing concentration risk. This would bring global consistency and efficiency to regulatory standards and reporting requirements across jurisdictions and provide increased assurances for financial institutions' use of third-party providers across borders.

However, the scope of any initiative to oversee third-party service providers would need to carefully consider the criteria for identifying such providers, and whether a third-party is already subject to existing regulatory requirements. This will allow for any initiative to be tailored accordingly, whereby consideration is given to whether the risk that the initiative seeks to address is already catered for as part of an existing regulatory regime.

Additionally, any direct oversight initiative should not become a barrier for competition in the market, eliminating the providers who cannot afford the costs of regulatory oversight and leaving only the big players in the market.

This global approach may also help reduce the risk of third-party restrictions and data localisation measures being introduced nationally, and regionally, which result in the need of financial institutions to fundamentally alter their outsourcing programs (such as cloud adoption strategies) and trigger increased costs and operational burdens. It would also bring benefits such as the efficiency and value of outsourcing regulatory reporting (such as registers of contractual arrangements), and the streamlined execution of specific oversight requirements by financial institutions and supervisors (such as on-site audits, whereby extensive time and resource of third parties are currently devoted to different audits, which are required under various fragmented regulatory frameworks).

The recent EU draft regulation, Digital Operational Resilience Act (DORA), is one example of a direct oversight initiative that is being considered. However, we believe that such regional approaches could pose significant challenges to financial institutions operating across borders. For example, limitations in one region may make the deployment of a global process to a certain service provider impossible. If regions diverge in their limitations regarding different providers then there may be no providers with which financial institutions could work on a global level. While outright bans remain unlikely, different approval processes or IT security requirements placed on the providers may result in regulatory risk that defeats the business case for such activities. Such an outcome would form a regulatory barrier to innovation and the modernisation of financial institutions' IT estates resulting in continued complexity, including greater reliance on end-of-life systems, and ultimately greater risk.

Q3. 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?

As a global and interconnected financial sector, we support effective cooperation and dialogue among financial institutions, third-party service providers and supervisory authorities. In particular, cross-border collaboration between regulators is necessary to realise regulators' legitimate right to access data for prudential supervision and to limit the risk of disparate

and potentially conflicting data access and sharing requirements imposed by different jurisdictions.

We believe that solutions for this cross-border data access challenge should be based on a globally interoperable mechanism to ensure continued interconnectedness, efficiency and resilience of the sector, as well as alignment with any global trade implications.

Suggestions of Collaborative Efforts

Regulatory Alignment and Coordination

We believe regulators can work more holistically with all parties to discuss the comments and inputs they regularly receive from financial institutions and service providers, and establish an overarching regulatory framework to address common challenges and reduce compliance costs and risks. These collaborative efforts may cover:

- establishing a common standard taxonomy for key terms and consistent principles for the adoption of an outcomes and risk-based approach;
- establishing voluntary standard contractual clauses between specific types of customers and service providers (e.g. financial institutions and cloud service providers);
- establishing an industry standard for service providers to be able to seek certification of approval from regulators (e.g. the MAS Multi-Tier Cloud Security (MTCS) Certification Scheme) and/or recognising a non-exhaustive list of industry standards against which providers can certify;
- leading the industry to develop a consortium for pooled audits of critical service providers; and
- develop coherent cross-border data sharing policies that do not jeopardise the efficient intra-group management of financial institutions

We also believe that better intra-regulatory communication to coordinate consultation and align the release and implementation dates of regulations will bring more certainty, and enable financial institutions to better plan and resource appropriately to ensure limited disruption of business-as-usual operations.

We note that, intra-regulatory dialogues should not be limited to those between financial regulators, but also regulators of other sectors as some challenges, such as digital issues that have an impact on the financial scope, may exceed the scope of financial regulations. Some of our members see a need for further coordination with regulators in different sectors and across countries to establish global solutions for the emerging issues in the digital landscape.

We also believe that a greater use of mutual recognition or equivalent arrangements will reduce the duplicating oversight of financial institutions for outsourcing and third-party relationships across their global footprints. For instance, local regulators could leverage the annual independent assessment and business continuity management testing for global service providers conducted by the headquarters of financial institutions instead of requiring local offices/branches to conduct the same.

Rehearsals of Disruptive Events

In the event of a disruption at a major provider, it is vital that the financial industry, including its regulators, have rehearsed some of the potential scenarios and steps required. Exercises that help all market participants better understand the actions they would need to take and pre-identify risks that could arise as a result would therefore be a useful initial step toward addressing concerns related to systemic concentration. Given the cross-border nature of the IT services provided it is likely that for a major failure of a provider such as a critical service provider, coordination between authorities would be necessary.

Channels for Collaboration

We suggest the below channels for executing the above collaborative efforts:

- **Public-private forums:** We encourage industry participants and policymakers across the globe to collaborate to identify potential risks and gaps in relations to outsourcing and third-party risk management, particularly given sector-wide interdependencies, and develop solutions to address the risks. This could assist with a number of the practical challenges identified in the Discussion Paper and this response, particularly in relation to ensuring that third parties across jurisdictions are aware of the regulatory environment in which financial institutions operate, and therefore help to combat common issues among both financial institutions and third parties.

- **Public consultation:** We may also leverage opportunities of discussing relevant topics, such as the BCBS' consultation on operational resilience, to bring to the table the broader discussion of risk management in relation to outsourcing and third-party relationships.

- **Global supervisory colleges:** We encourage market participants to form global supervisory colleges or crisis management groups to develop a framework for managing issues like digital operational resilience.

- **Supervisory information sharing and collaboration:** In order to contribute to globally consistent regulatory and supervisory approaches to outsourcing and third parties, we encourage establishing a mechanism for supervisory information sharing and collaboration. This could help combat issues in relation to common terminologies, scope, standards, measurement of cross-border concentration risk and data access.

    - In particular, maintenance and sharing of outsourcing registers, which recognise the entire cascade of outsourcing would do much to create clarity and transparency. However, we maintain that every register should build on existing registers, and there should not be any new requirements for financial institutions to maintain institution registers. There should be a very clearly defined, narrow group of institutions/people granted access to those registers.

    - As mentioned above, where it involves intra-group outsourcing, a home-to-host information sharing platform may assist in addressing some of the risks perceived by local regulators in relation to the exercise of their supervisory function and their ability to obtain necessary information on the outsourced or third-party service.

Q4. 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?

We set out a number of key lessons our members have learned from the COVID-19 pandemic as follows:

- One of the key lessons for financial institutions is to adopt a risk-based approach and focus on operational resilience in managing outsourcing and third-party risk exposure. COVID-19 has shown the world that operational resilience and business continuity management should cover "severe but plausible scenarios" (in particular, events which occur in waves, against which financial institutions must prepare for the next wave of risks, rather than solely the immediate impact).

- Where there is an incident of failure, it is important that time of recovery is documented properly according to written procedures. There should be in place proper mechanisms for reporting to relevant governance committees.

- A vendors' business continuity management testing is as equally important as financial institutions' own business continuity management planning and testing. If financial institutions solely focus on service providers' achievement of service levels, by the time risk incidents manifest themselves in SLA deterioration, it would be too late for financial institutions to react to the third-party failures that disrupt their operations. In assessing third-party vendors' performance, the key performance indicators should, among other

requirements, also measure the status of the service provider's infrastructure, key personnel and financial status..

- The pandemic has shown that many manual processes could be automated or digitized by using new or emerging technology (e.g. artificial intelligence, distributed ledger technology, etc.). The increasing demand of technology use will likely deepen financial institutions' partnerships and relationships with third-party service providers.

- Specifically, in terms of managing operational resilience, we observe from COVID-19 that cloud has emerged as an important tool for enhancing financial institutions' operational resilience as some prominent cloud service providers can offer a robust IT environment at a reduced cost.

- Short-term solutions developed due to the pandemic may turn into long-term solutions within the 'new normal' which may require business operations to adapt how they manage risk both internally and with third parties. For instance, work-from-home has become common place in light of global lockdown policies and might impact future working culture.

- COVID-19 has also made financial institutions realise that their performance of control functions must be more dynamic to cope with exceptional circumstances. For instance, they have to be prepared and equipped to conduct internal audit assurance testing and exit plan execution under stressed scenarios when travelling is not possible. Further, where feasible, members have successfully utilised remote modes to conduct supplier control assessments due to restrictions on travel and personal interaction.

- COVID 19 also highlighted the need for exit plans/exit strategies in respect of critical outsourced arrangements to set out sufficient level of detail for the effective transition of services (including, in respect of the migration of data).

- Additional coverage and frequency of financial due diligence and monitoring for certain suppliers (e.g. monitoring their risk profiles) helped increase the transparency of suppliers' financial health.

- In respect of internal risk management, appropriate considerations should be given to risks related to health and safety, infrastructure limitations, as well as how to reduce absence levels and increase productivity.