asifma

Growing Asia's Markets

20 April 2026

ASIFMA Response to MAS Consultation Paper on Proposed Guidelines on Third-Party Risk Management

On behalf of the Asia Securities Industry & Financial Association ("**ASIFMA**")[1], representing our Financial Institution and Asset Management members (together, "**FI**")[2], we are pleased to respond to the Monetary Authority of Singapore's ("**MAS**") Consultation Paper on Proposed Guidelines on Third-Party Risk Management (the "**Guidelines**"). This submission has been prepared with the support of ASIFMA's Law Firm member, Allen & Gledhill.

Q1. MAS seeks comments on proportional implementation of the Guidelines. Where respondents envisage challenges in observing specific expectations on a proportional basis, respondents are encouraged to propose alternatives to the drafting of the expectations and the rationale for doing so.

While we acknowledge the increasing reliance on external providers and the need to address risks and dependencies from arrangements that do not fall within the scope of the definition of "outsourcing arrangements", the expanded scope significantly increases the volume and diversity of arrangements that will fall within the Guidelines. We appreciate MAS' incorporation of proportionality and materiality to calibrate regulatory expectations, and note that several areas of the Guidelines reflect this proportionate approach. Nonetheless, given this expanded scope, we are of the view that it is important that proportionality is applied consistently and explicitly across the Guidelines to ensure it remains operationally feasible for FIs to implement the Guidelines while achieving sound risk management of third-party arrangements.

As such, we respectfully request for:

(i) a clearer differentiation between baseline expectations for all third-party arrangements and enhanced requirements for material third-party arrangements, with controls and oversight tailored to the level of risk and impact. This would help ensure that more intensive controls are applied to material third-party

[1] ASIFMA is an independent, regional trade association with over 150 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, and competitive 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. More information about ASIFMA can be found at: www.asifma.org.

[2] ASIFMA Membership Composition: https://www.asifma.org/membership/members/

ASIFMA Headquarters
Unit 3603, Tower 2, Lippo Centre
89 Queensway
Admiralty, Hong Kong
Tel: +852 2531 6500

ASIFMA Singapore Office
12 Marina View, Asia Square Tower 2
Level 11, #11-01
Singapore 018961

arrangements where the underlying operational or resilience risks are greatest, and FIs are compliant with the Guidelines (such that MAS need not take action under paragraph 2.5 of the Guidelines). For instance, it could be clarified that joint business continuity and disaster recovery testing is not required for non-material arrangements.

(ii) a stronger linkage between certain requirements and the level of risk or potential impact – particularly, that the Guidelines take a stronger outcomes-based approach to best operationalise the envisioned proportionate, risk-based approach – an approach that underpins TPRM regulatory frameworks globally. This would entail more explicitly scoping material third-party arrangements primarily based on impacts (specifically, the role of those arrangements on the safety, soundness and resilience of the FI). This would allow FIs to dedicate enhanced oversight and resilience-related controls (such as business continuity planning and testing), and focus necessary resources and expertise to where risk is most likely and impactful to the FI, its clients and the broader Singapore market.

(iii) distinction between (a) third-party arrangements where the FI is the direct contracting party; and (b) arrangements where services are provided to the FI under a group-wide operating model, with contractual relationships and key controls exercised by a parent or affiliated entity. We recognise that FIs remain accountable for risks arising from services they rely on, even where such services are provided under group or intragroup arrangements. In this regard, as an FI is subject to the Guidelines where such group or intragroup arrangements support or impact the FI's operations or regulated activities), we seek confirmation that the group / intragroup nature of the relationships (where there is more limited unilateral contractual control over the underlying service provider) can be taken into consideration in the extent of compliance with the Guidelines (with guidance on such extent, as described below).

Global FIs

We note that the Guidelines acknowledge (at FN 12) that local FIs with overseas head offices may leverage global or group-wide frameworks, subject to their alignment with the Guidelines and appropriate local supplementation. To further support MAS' objective of delivering a proportionate and effective framework, this concept would benefit from being more clearly articulated in the main body of the Guidelines to ensure it is understood as a general principle application. We therefore recommend that MAS explicitly provide that, where appropriate (e.g. for risk assessments, due diligence and control frameworks set out in section 6 of the Guidelines), FIs may rely on group-wide frameworks, governance structures and control environments in meeting the expectations in the Guidelines, including in the context of intragroup arrangements and where control resides at the group level. Allowing reliance on group frameworks, on a proportionate basis and with appropriate local oversight and accountability, would support consistent and efficient implementation while reflecting the reality of established operating models for global FIs

and remaining aligned with MAS' objectives. This would be in line with the global nature of third parties, where the daily oversight is likely managed elsewhere in the FI. For example, local boards and senior management should be permitted to evidence effective oversight through mechanisms such as periodic reporting, escalation protocols, supplemental local risk assessments which focus on Singapore-specific risks and regulatory considerations, and supplemental local guidance, rather than being required to independently approve or re-establish all elements of the TPRM framework. In addition, where appropriate, FIs should have the flexibility to exercise oversight at a portfolio level, including monitoring of key themes such as exceptions, delays, and other material issues with escalation where necessary. This approach ensures alignment and maintaining operational practicality.

Similarly, for intragroup service providers, we seek express confirmation that such service providers may generally be subject to a lighter-touch approach – for example, in relation to risk assessments, intragroup service providers should subject to more simplified risk assessments. This is because intragroup arrangements differ in substance from external third-party engagements in several respects, including: (i) shared governance frameworks, policies, and risk management standards across the group; (ii) greater transparency, oversight, and escalation channels within the same corporate group; and (iii) alignment of incentives and reduced risk of opportunistic behaviour as compared to external service providers. Hence, requiring the same depth and granularity of risk assessment for intragroup arrangements as for external third parties may result in unnecessary duplication, without a commensurate improvement in risk outcomes. This may also impose disproportionate operational burden on FIs, particularly where the intragroup services are long-standing, stable, and subject to group-level assurance.

There are two viewpoints on MAS' approach of proportional implementation of the Guidelines, and the extent and degree to which an FI implements the expectations in the Guidelines should be commensurate with the size and complexity of the FI. Some non-bank members have business models which are very different in scale and risk from banking business models. They suggest that non-banks should be able to consider the obligations in light of their business models. This is on the basis that non-banks do not operate payment, deposit taking and (where applicable) retail banking infrastructure that could be more impacted by third-party service providers. Non-bank FIs, including asset managers, do not pose the same risks in these areas and should therefore be subject to proportionately less obligations by default. Hence, a similar approach to the current outsourcing guidelines, which distinguishes banks from non-banks, is preferred. Yet, for some banks, harmonisation of Guidelines across FIs is preferred, with proportionality applied within a single, consistent set of expectations. This is because distinction may create unnecessary complexity, particularly for FIs operating both bank and non-bank entities.

However, to the extent that the MAS takes a harmonised approach such that the standards for TPRM apply to banks and non-banks, it is respectfully submitted that paragraph 2.1 of the Guidelines should be amended as follows:

> "2.1 The extent and degree to which an FI implements the expectations in these Guidelines should be commensurate with the size and complexity of the FI and the nature of risks in, and materiality of, the third-party services the FI uses. ***In particular, the application of requirements to non-bank institutions should be proportionate and reflect differences in business models, including through the appropriate calibration of the scope, depth and frequency of risk management and oversight of third parties***."

This would ensure that the application of the Guidelines explicitly and appropriately reflects differences in the nature and risk profile of non-bank FIs, which may not present the same level or type of third-party risk across all areas, while maintaining a consistent and harmonised underlying framework.

<u>Material third-party arrangements</u>

The definition of "material third-party arrangement" plays a crucial role in ensuring the envisioned framework remains proportionate and directs specific measures/activities to arrangements which truly require enhanced risk management across the full TPRM lifecycle. Ensuring this definition more accurately scopes these arrangements is paramount to the success of a TPRM regulatory framework.

The current definition of a "material third-party arrangement", however, relies on a combination of trigger events and broadly scoped potential considerations, which would result in a wide range of arrangements being captured that do not pose the type of impact that are best addressed through the proposed enhanced requirements, such as joint testing. In a framework that applies to all third-party arrangements, such a definition risks extending requirements designed for higher-risk arrangements to a much broader set of lower-risk relationships.

To support the effective application of a risk-based framework, the definition of material third-party arrangements – and the related concept of material subcontracting arrangements – should remain clearly targeted to only capture arrangements that pose a genuine risk of material operational, resilience or customer impact and ensure industry consistency. An overly broad scoping has already been observed under the existing outsourcing regulatory framework and would become unmanageable if carried over to a broader third-party scope (outsourcing + non-outsourcing), without revision to ensure a more effective outcomes-based approach. In this regard, we appreciate MAS' incorporation of the key elements of international standards, and respectfully request that MAS further aligns its expectations with international standards where appropriate.

The definition of "material third-party arrangement", whilst carried over from the definition applicable to banks currently in the existing Outsourcing Notices, risks inappropriately pulling in a very large number of relationships into scope as 'material' and undermining MAS' proposal for a proportionate framework. Such an approach could lead to risk management efforts being diverted to third-party services which do not pose genuine risk to FIs and its customers or the Singapore financial system, and away from managing the real risks.

Specifically, we set out the following comments in relation to the definition of "material third-party arrangement":

(i) In relation to sub-paragraphs (a) to (c) of the definition, which set out certain "trigger events", such as any unauthorised access to any information, or any unauthorised disclosure – the factors set out in sub-paragraphs (a) and (b), while relevant and important, are broad (e.g., risks such as unauthorised access may arise across a very wide range of service providers, as many service providers process or host information in some form). Including them as triggers within the materiality definition risks vastly expanding the population of arrangements that could be classified as material. Moreover, such risks are more appropriately addressed through cyber, data governance and due diligence controls – as in current practice – and should not necessarily determine whether an arrangement is considered material in the prudential or operational sense. We therefore respectfully request removing the proposed triggers and instead focussing materiality on the impact of a failure or disruption of the arrangement (i.e., outcomes-based focus), rather than the presence of a broader range of events.

(ii) in relation to the phrase "will materially affect adversely or is likely to materially affect" – the inclusion of "or is likely to" materially affect significantly lowers the threshold by capturing potential or theoretical impacts – leading to an over-classification of material arrangements (increasing governance and oversight burdens without necessarily reflecting genuine operational dependency). By contrast, the term "will materially affect adversely" emphasises actual, significant impacts. We therefore suggest "or is likely to" is deleted to ensure the concept of materiality remains targeted. We note that the current definitions applicable to banks and non-banks already encompass an element of "potential" or "likely" – however, in the context of all third-party service providers, it is respectfully submitted that this would be too broad.

(iii) most importantly, in relation to sub-paragraphs (i) to (iv), the criteria are drafted broadly and risk significantly expanding the population of arrangements classified as material, beyond those that represent genuine operational, resilience or prudential risks. This overly broad scope is compounded when considered in connection with the inclusion of triggers covering: *any* information held by the

service provider or sub-contractor; and the books, systems or premises of the service provider or sub-contractor. We respectfully request that the impact assessment focuses on where a failure or disruption would have a materially adverse impact on the FI – for example in terms of safety and soundness, operational resilience or customer outcomes. In particular:

(a) paragraphs (i) and (ii) – these are framed broadly and could capture a very large number of arrangements under an expanded third-party scope. We recommend that these criteria be removed so that the impact assessment focuses on resilience risk or customer outcomes. A potential compromise could be to retain but combine the considerations (i.e., makes these an "and" instead of an "or") for (i) and (ii) so they better capture higher impact scenarios, e.g.: "the provision of a financial service by the FI and creates significant impact to the customers or any group of customers, financial soundness or reputation of the FI". This would maintain MAS' considerations but more accurately scope those considerations based on impact/outcome.

(b) paragraph (iii) refers to the ability of the FI to manage the risks arising from the service, rather than the impact of the service itself on the FI's risk profile and related risk appetite. This creates a much lower and more subjective threshold, as many services could indirectly affect the FI's ability to manage legal, reputational, technology or operational risks, even where the service is itself not material. We respectfully request that this provision is removed or amended to refer to "the ability of the FI to remain within its risk appetite" – this again would help maintain MAS' considerations but more closely focus on impact/outcome.

(c) paragraph (iv) refers to the ability of the FI to comply with all laws and regulatory requirements, which could apply to a very wide range of third-party arrangements given the range of various laws under which the sector operates (e.g. employment law, tax law, environmental rules). While this is clearly an important consideration in an FI's broader risk and control frameworks, it conflates regulatory compliance, which is important, but not the same as consideration of impact to the firm or its clients. As result the current language introduces a low threshold for materiality. We note that similar concerns were raised on the BCBS TPRM Principles and the FSB TPRM Toolkit. Following industry feedback, the final text was amended to refer to key laws and regulations, which allows for reflection on potential impact to the firm and its clients. Consistent with that approach, we respectfully request that MAS limit the reference to key laws and regulatory requirements, in order to maintain a more targeted materiality threshold and alignment with international frameworks.

To best capture the above recommendations to apply an outcomes-based approach that better focuses materiality on impact, the amended "material third-party arrangement" definition would read as:

"material third-party arrangement" means a third-party arrangement where the FI has reasonable grounds to believe that

~~(a) any unauthorised disclosure of, access to, collection of, copying of, modification of, use of, disposal of or acts with similar risks done in relation to, any information, held by the service provider or sub-contractor, as the case may be;~~

~~(b) any unauthorised access to the books, systems or premises of the service provider or sub-contractor, as the case may be; or~~

~~(c)~~ a **disruption or** failure by the service provider to provide the relevant service in accordance with the third-party service agreement,

will materially affect adversely ~~or is likely to materially affect adversely~~

(i) the provision of a financial service by the FI **and** ~~(ii)~~ the customers or any group of customers, financial soundness or reputation of the FI;

(iii) the ability of the FI to **remain within its risk appetite** ~~manage its risks (including legal, reputational, technology and operational risks) arising from the service~~; or

(iv) the ability of the FI to comply with **key** ~~all~~ laws and regulatory requirements that apply to the FI, whether in Singapore or elsewhere.

Interaction with existing framework

The Guidelines introduce a broader TPRM framework while the existing Notices on Management of Outsourced Relevant Services remain in force. While this approach is understandable as part of a transition, it results in a layered framework in which FIs will need to apply similar but not fully aligned requirements to the same group of arrangements – including maintaining parallel or duplicative reporting processes and templates for registers (see our response to question 3 below). This risks diverting effort towards classifying arrangements as outsourcing and non-outsourcing and towards reconciliation of frameworks, rather than strengthening underlying risk management.

Over time, greater alignment between the Guidelines and the existing Notices would support the objective of a proportionate and coherent TPRM framework. In the interim, we suggest that register processes and reporting templates are consolidated to significantly reduce operational complexity. We also seek clarification on the intended approach to the

existing Notices, and whether these will be revised or aligned with the new Guidelines to ensure that the framework can operate as a single, holistic TPRM regime.

Q2. MAS seeks comments on the expectations applicable to FIs with a branch or subsidiary under them and which are (i) subject to consolidated supervision by MAS or (ii) owners of a critical information infrastructure.

We seek confirmation that the Guidelines will not apply to foreign entities that:

(a) are not regulated by MAS;

(b) are not the branch or subsidiary of an entity in Singapore that is regulated by MAS (e.g. head offices that are incorporated overseas, with branches that are established and regulated in Singapore); and

(c) are not regulated and are entities in which banks hold a major stake that is approved by the MAS under section 32 of the Banking Act 1970 of Singapore.

Where an FI has a branch or subsidiary overseas, and is required to ensure that the Guidelines are observed by that branch or subsidiary, we highlight that application of the Guidelines across jurisdictions may require a longer transition time due to local legal and regulatory constraints, contracting norms and differing definitions (e.g., "critical information infrastructure" may differ by country and local operating context). We note that the proportionality principle will apply across the FI's branches/subsidiaries, which will make assessments in accordance with their jurisdictional and local contexts.

In addition, where the relevant offshore laws governing the FI's head office or parent could potentially have legal restrictions on other regulators' direct rights to audit the FI's head office or parent (for example without going through a legal process to do so), it is respectfully submitted that FIs should be permitted to take these legal conflicts into consideration and provide for mitigating controls such as independent assurance reports, enhanced monitoring and alternative evidence.

Q3. MAS seeks comments on (i) the proposed register template to be submitted to MAS; (ii) the main categories of third-party services that FIs are currently utilising and monitoring internally, which will be consolidated across the industry for inclusion in the register accordingly; and (iii) whether ISO-3166-2 should be used to collect location information.

(i) Proposed Register Template

We support MAS' objective of improving visibility into concentration and dependency risks across the sector. We also support MAS' proposal to introduce a standardised register of third-party arrangements, as it enhances transparency, facilitates supervisory oversight and promotes consistency across the industry.

Information included in the "Third-Party Register" tab of Annex B (the "**Register**")

We are supportive of MAS's objective to harmonise third-party reporting requirements and templates (including across existing Notices in due course). Registers are inherently resource-intensive tools and therefore it is important that their design remains operationally feasible and proportionate, and focused on delivering meaningful supervisory insight. Regarding the application of proportionality within the proposed reporting framework, this should ensure that the nature of information required is calibrated appropriately for non-bank FIs.

Preliminarily, we respectfully request that MAS reviews the information collected from banks since the current outsourcing register took effect, and reduces the information required, as not all information fields may serve the purpose(s) that the MAS had intended when the template was issued – particularly, please see our comments on columns N to P of the Register below.

In addition, we would invite MAS to consider introducing a pilot phase of the Register to (1) support FIs in preparing for implementation and address any practical implementation challenges ahead of the first submission cycle; and (2) for MAS to understand the level of data that FIs are realistically able to provide.

We respectfully request that data fields be streamlined so that those that are unnecessary, duplicative or disproportionated can be removed. We highlight that some fields will be "not applicable" or "not available" for certain third-party arrangements. Particularly, information required under columns N to P (Jurisdiction, Cities, and Customer Information) and columns AD and AE (information on service providers'/ material sub-contractors' business continuity plan) may not be available, especially where services are provided by intra-group entities (e.g. Head Office) or third-party providers that rely on multi-layered outsourcing or cloud infrastructure. In this regard, please also see our response to question 10 of this Consultation Paper.

In this regard, the form of the Register could be the subject of further discussion with the MAS – some members suggest the following for MAS' consideration:

(i) streamlining the Register for non-bank FIs or bank FIs with simpler business models, and flexibility for non-bank FIs or bank FIs with simpler business models to adopt the bank FIs Register so that the non-bank entities or the bank entities with simpler business models within bank FIs can leverage one integrated infrastructure to streamline reporting; and

(ii) using a different inventory format (on the understanding that the required vendor-related details would be included).

In terms of the coverage of the Register, members agree with its scope being explicitly limited to material third-party arrangements (and the reporting of non-material arrangements is not required but may be included). Otherwise, significant and unnecessary complexity would be introduced where the objective should be to (i) harmonise reporting requirements and templates across all material third-party arrangements for both banks and non-bank FIs; and (ii) to streamline data fields that are seen as unnecessary, duplicative or disproportionate.

More specific comments are discussed below on the basis that the Register is geared towards recording material third-party arrangements. On the basis that only material third-party arrangements are required, a single register without differentiation between material vs non-material third-party arrangements is supported by some members.

Regardless, as specified above, piloting the Register with the industry would give a better understanding of the practical implications of the relevant fields being completed and whether any flexibility can be applied depending on proportionality and business complexity. In addition, we respectfully request for phased implementation, including an initial phase where the Register may not be fully complete, with full completeness of data being achieved only after one or two reporting cycles.

Refinements to the Register

To further support an approach that is operationally feasible for firms while also providing meaningful supervisory insight, we respectfully make the following comments and request the following refinements to the Register.

For groups with more than one entity subject to the Guidelines, we suggest that the Register should be submitted in a single consolidated file by introducing an "Entity" column in the Register. This approach streamlines validation processes and minimises inconsistencies and errors associated with maintaining multiple files.

In relation to rows 4 and 5 of the "Instructions" tab of Annex B: We note the distinction drawn between ongoing and non-ongoing third-party services. However, as currently drafted, the reference to non-ongoing arrangements involving the disclosure of customer information could be interpreted as expanding the scope of the register beyond material third-party arrangements. We recommend explicitly limiting this expectation to material third-party arrangements, including in the context of non-ongoing services. This would avoid any unintended broadening of scope and ensure the Register remains focused on arrangements that are most relevant from a supervisory perspective.

In relation to column C of the Register ("Is this an ongoing third-party service?"): The purpose and applicability of this column are unclear for non-bank FIs. FN 5 of the Consultation Paper states that, in the case of banks and merchant banks, the Register

should include: (i) all ongoing outsourced relevant services obtained or received from a service provider; and (ii) all outsourced relevant services involving the disclosure of customer information, as set out in paragraph 3.1 of MAS Notices 658 and 1121 on Management of Outsourced Relevant Services. Given that this clarification is explicitly framed in the context of banks and merchant banks, we seek confirmation that non-bank FIs are not required to complete Column C. If non-banks are required to complete Column C, it would be helpful for MAS to clarify whether the distinction between ongoing and non-ongoing third-party services is intended to result in different regulatory expectations, supervisory focus, or risk management requirements. If MAS expects FIs to treat ongoing third-party services differently from non-ongoing arrangements, we suggest that such distinctions and their implications be explicitly articulated in the Guidelines, as there is currently no guidance explaining how this classification should be applied or used.

In relation to column L of the Register ("Service provider/material sub-contractor supports the delivery of Critical Business Services to meet relevant Service Recovery Time Objectives"): To ensure this requirement remains proportionate and aligned with the proposed Register's scope, this data field should be explicitly limited to material third-party arrangements. Capturing service providers and sub-contractors that play a meaningful role in the delivery of a Critical Business Service would provide more meaningful and targeted supervisory insight.

In relation to columns N to P (i.e. Jurisdiction, Cities, and Customer Information) of the Register: We do not see a benefit in requiring FIs to report location at country, jurisdiction and city level. While country-level information provides meaningful insight into geographic and jurisdictional risk, the additional requirement to specify jurisdiction and cities is unlikely to enhance supervisory value and introduces unnecessary complexity (and regulatory burdens) – particularly given the expanded scope of arrangements to be reported, and for services delivered across multiple or dynamic locations. If the purpose of collecting such information is to assess geography concentration, we recommend that MAS allows FIs to provide a summary by country or city, instead of for each third-party service; in this regard, we are also happy to provide other alternatives if MAS is able to share its purpose for collecting such information. Otherwise, we recommend deleting column O and streamlining the requirement in Column N to focus on country-level reporting. Alternatively, we respectfully request that MAS allows primary location reporting where precise granularity is not available, and reliance on service provider disclosures for such information. Should MAS decide to retain column O (without allowance for primary location reporting), we note that cloud-based services and globally distributed processing environments may not map neatly to fixed sub-national location codes, especially where data residency is dynamic or workloads are distributed across multiple regions. Thus, we respectfully request that MAS allows FIs to populate the column O with standard descriptors such as "multi-location / distributed" (with optional qualifiers like "distributed

- global" or "distributed - [region]"). This would preserve supervisory value by maintaining visibility of cross-border exposures while acknowledging operational constraints.

In addition, we note that the current structure requiring the reporting of certain information across multiple tabs could be directly captured by having FIs list the jurisdictions in a single row within the Register to reduce the need for cross-validation across multiple tabs, duplication and potential inconsistencies. However, this approach is only workable if the current row limit is addressed, otherwise FIs may not be able to accommodate reporting all legal entities, countries, cities etc. in the same tab. If separate sheets must be maintained, we propose that only key reference fields – specifically columns A, E, F and G are required to be populated in tabs "Col N – Jurisdictions", "Col O – Cities", and "Col P – Cust_Info", as the information contained in column B to column F of those tabs can be referenced from the Register.

In relation to Column Z ("Was there a change in materiality following the most recent materiality assessment performed for the third-party arrangement?") of the Register: Given that the register is limited to material third-party arrangements, any change in materiality would already be reflected in the composition of the Register itself. For example, where an arrangement is no longer material, it would fall out of scope and no longer be reported. Conversely, where an arrangement becomes material, it would be captured through notification and included in the Register as a new entry in the relevant reporting cycle. This requirement therefore appears redundant and should be deleted.

In relation to the question in column AF of the Register ("whether an arrangement is an outsourcing or non-outsourcing third-party arrangement"): We do not see a benefit in requiring firms to classify arrangements as "outsourcing" or "non-outsourcing" as this would create another layer of classification and it is not clear that such additional classification would be meaningful. The Guidelines do not define outsourcing and the distinction does not meaningfully support risk management or supervisory outcomes – particularly as risk management expectations are aligned across third-party arrangements. As the MAS framework evolves towards a more holistic TPRM approach, this distinction will become increasingly arbitrary and risks introducing unnecessary complexity. We therefore propose removing this data field in the interests of a more streamlined and proportionate Register. However, should MAS decide to retain this column, we respectfully request that MAS includes a clear definition of an "outsourcing arrangement" in the context of the new third-party arrangements definition, together with the relevant qualification criteria, within the Guidelines. This is because, once the Guidelines are issued, non-bank FIs will no longer have any clear definition of an "outsourcing arrangement". If this column is retained, we would be grateful for clarification on the regulatory purpose and intended use of this classification in the framework of the Guidelines, and as mentioned above, would respectfully request that this data field be removed.

In relation to columns S, T and U of the Register (Name and Business registration number of alternate service provider; and Country or Jurisdiction where the alternate service provider is registered): We recognise that for material arrangements, FIs should maintain credible substitution and exit strategies, which may include identifying alternative service providers where appropriate. However, it is not standard practice for firms to maintain additional identifiers such as BRNs or jurisdictional details. We suggest limiting this requirement to providing the name of the alternate service provider, or otherwise making the additional fields (columns T and U) optional.

In relation to the category "Management of policy issuance and claims operations by managing agents" (set out in cell A24 of the "Drop-down Data" tab of Annex B), we seek clarification on whether this category refers to group insurance policies purchased by FIs as part of staff benefits or if this applies only to FIs that are insurers that engage third parties for insurance policies that they issue. If this relates to group insurance policies purchased by FIs are part of staff benefits, we seek clarification on the following:

(i) whether this category is considered an outsourcing or non-outsourcing third-party arrangement (under column AF of the Register); and

(ii) if this category is considered an outsourcing arrangement, which Annex of MAS Notice 658 would this category fall under – particularly, whether it is intended to be treated separately from "Services relating to manpower management, including but not limited to payroll processing, benefits and compensation administration and recruitment" currently set out in Annex C.

Non-material third-party arrangements

To the extent that any non-material third-party arrangements are recorded as good practice, some members request generating a separate and more simplified register for third-party arrangements which are not classified today as outsourcing arrangements, or are lower-risk third-party arrangements – this is because data fields relating to audit and BCP may be challenging to obtain for (what today are classified as) non-outsourcing arrangements. This also reflects the current transitional state of the third-party risk management framework – moving from a layered approach (i.e. outsourcing versus non-outsourcing and material versus non-material) towards a more unified model where materiality is the primary differentiator. At this stage, adopting a single register subject to differing requirements may introduce unnecessary complexity and variability, and having a more simplified register for lower risk third-party arrangements with clearer alignment to their respective requirements would support a cleaner and more effective reporting approach. However, as non-material third party arrangements are not required to be included in the register, this simplified register would not be a mandatory requirement.

Particularly, in relation to columns AA and AB of the Register ("FI's frequency of audit on the service provider / material sub-contractor (Year(s))" and "When was an independent

audit last conducted on the service provider / material sub-contractor?"): For non-material and lower risk arrangements, such audit requirements and frequencies are not typically defined today given their nature and risk profile. We note that the register is to be completed only for material third-party arrangements. We would respectfully request that such requirements do not apply across all third-party arrangements because this would require a significant uplift in governance, monitoring process and resources. In this regard, we suggest that mandatory audit requirements and frequency expectations be primarily applied to material third party arrangements with flexibility for non-material third party arrangements based on a risk-based approach. This would also support alignment with other international practices (e.g. European regulatory frameworks) where audit requirements are more applied to material while allowing proportionality for non-material arrangements.

Arrangements included in the Register

We understand that the Register should minimally include all material third-party arrangements, and is meant to support an FI's effective management of third-party risks, by ensuring that the FI can "map dependencies and interconnections relating to its material third-party arrangements, where possible" (per paragraph 3.6(c) of the Consultation Paper).

We note that there may be a duplication in terms of the reporting of non-material intragroup services in the Register vs the reporting of foreign related corporations (FRC) – essentially these services are in the form of business collaboration / coverage sharing arrangements within an FI, which are already tracked and reported for FRC purposes. Hence, we respectfully request for such services to be excluded from the Register to avoid duplicative effort and requirements.

Sub-contractors

We are supportive of the position that information on material sub-contractors should be provided "where possible" (as per paragraph 4.3 of the Guidelines) as this would allow FIs to rely on available disclosures, group-level confirmation, vendor due diligence and assurance reports.

(ii) Main Categories of Third-Party Services that FIs are Currently Utilising and Monitoring Internally

We suggest harmonising the categories with other relevant regulations such as the EU Digital Operational Resilience Act (DORA) and UK PRA/FCA (PS26/2: Operational Incident and Third Party Reporting), as this alignment will help reduce the compliance burden on FIs by minimising the need to collect and report jurisdiction-specific, bespoke data points.

More generally, we would highlight the risk that the prescribed categories may not adequately capture the breadth and nuance of services used by large international FIs, and seek guidance on the types of activities that commonly constitute a significant portion of such registers, to assist FIs in determining third-party services classification and enhance industry consistency. We also respectfully request for flexibility for FIs to map services according to their internal classifications.

Separately, we request for examples of what today would qualify as non-outsourcing arrangements that still fall within the scope of third-party arrangements.

In relation to situations where a single third-party service provider spans multiple categories in the proposed taxonomy, we respectfully request that FIs may generally maintain one register entry per third-party arrangement (i.e. per contractual service relationship), and indicate multiple applicable categories in Column B where relevant. Separate entries should be required only where services are provided under separate contracts or are otherwise operationally distinct (e.g. different delivery locations, different materiality assessments, or different risk ownership), such that separate oversight and reporting is warranted. This will ensure comparability and avoid double counting.

(iii) Whether ISO-3166-2 Should be Used to Collect Location Information

Some members do not recommend adopting ISO3166-2 at this stage, as the coding standard is not commonly used across all FIs and it may increase reporting burden without materially improving risk insights.

Other members are supportive of adopting standardised country-level codes such as ISO 3166-2, to support greater consistency and interoperability of reporting. To minimise implementation burden, such codes should be pre-populated within the Register template. The related proposal here is to remove city-level reporting, to ensure the overall approach remains proportionate and operationally feasible. To that end, we also note that ISO 3166-2 is a standard for country subdivisions (e.g. states/provinces/regions) rather than cities, and for certain cloud-based services and globally distributed processing environments, ISO 3166-2 may not always map neatly to cities or sub-national location codes.

Should MAS decide to retain city-level reporting, the members that are not supportive of adopting ISO3166-2 further suggest that MAS should permit the use of city names (e.g. London) for location reporting purposes as most FIs record this information in full.

Q4. MAS seeks comments on the proposed frequency of submission.

We suggest requiring FIs to submit the register annually (instead of semi-annually) to reflect a more proportionate approach and alignment with international standards (consistent with MAS' objectives) and global regulatory approaches (e.g. the EU Digital Operational Resilience Act (DORA), PRA/FCA (PS26/2: Operational Incident and Third Party Reporting), and APRA (Prudential Standard CPS 230 Operational Risk Management). A semi-annual submission frequency would create significant operational burden without a commensurate benefit to risk management or supervisory outcomes – particularly given the expanded scope of arrangements captured under the framework. Given that material changes are already subject to event-driven escalation, the incremental risk benefit of semi-annual reporting appears limited. Moreover, in practice, an FI's third-party population and associated risk profile is unlikely to change materially within a six-month period, and any significant changes would typically be captured through existing notification processes. Further, most data fields are likely to only be refreshed annually, through annual due diligence cycles, including independent audits and business continuity exercises (e.g. column Z, "Was there a change in materiality following the most recent materiality assessment performed for the third-party arrangement?"). As such, a mid-year submission is unlikely to provide materially new insights. A shift to a semi-annual register would be overly frequent given the operational effort required to gather and validate information across multiple service providers.

Q5. MAS seeks comments on the proposed responsibilities of board and senior management in managing third-party risk.

We note that some of the requirements are prescriptive and conflate roles and responsibilities of the board and senior management, and respectfully recommend the following:

(i) Paragraph 5.5(c) requires the board to define "appropriate approvers", and paragraph 5.5(e) sets out an expectation that the board should ensure that senior management establishes specific TPRM governance structures and processes for risk management. Such responsibilities blur the distinction between the board's oversight role and senior management's responsibility for implementation. Consistent with industry advocacy on the BCBS TPRM principles, we recommend clarifying that the Board's role is to provide effective oversight of the framework, while responsibility for establishing and operating governance structures and processes should remain with senior management. This would better reflect established governance practices.

(ii) The expectation set out in paragraph 5.6(g) of the Guidelines should not be interpreted as requiring FIs to have contingency plans in place and tested for all third-party arrangements. In practice, this level of recovery strategy would only be appropriate for resilience-critical arrangements. We recommend that this requirement be framed to reflect that senior management is responsible for

ensuring that "contingency plans for material third-party arrangements where a disruption would have a material impact on the FIs ability to deliver a critical business service, based on realistic and probable disruptive scenarios, are in place and tested".

More generally, in relation to paragraph 5.5 of the Guidelines, we note that (1) documented board-level endorsement, in a form consistent with the FI's governance arrangements, should be sufficient to meet the approval requirements under that paragraph; and (2) a consolidated annual board approval of an overarching third-party risk management policy and framework should be sufficient to meet these obligations without requiring separate approval for each item. We note that a consolidated approach of this kind is operationally proportionate and consistent with the objectives of the Guidelines, whilst preserving the substance of board accountability.

In relation to paragraph 5.6(b) of the Guidelines, we seek non-exhaustive examples on the roles and responsibilities expected for risk management of third-party arrangements (in particular for line 1 and 2 functions) to distinguish ownership, oversight, and governance accountability. This would support clearer operating models across the lines of defence, while allowing FIs flexibility to allocate responsibilities in a manner that reflects their business, technology, and risk management arrangements, especially in areas that require timely decision-making and ongoing operational responsiveness.

More generally, we seek confirmation that the expectations are outcomes-focused, such that there is no need for any specific standalone governance structures.

Q6. MAS seeks comments on the proposed expectations on governance, risk management and strategy.

The requirement to maintain a documented third-party risk strategy is broadly consistent with existing expectations and international standards. However, the Guidelines set detailed expectations as to the content of the strategy and the matters that must be explicitly addressed. We recommend MAS take an outcomes-based approach, allowing FIs' flexibility in developing the contents of their third-party risk strategies.

In relation to paragraph 5.9 of the Guidelines:

(ii) sub-paragraph (b) – we seek clarification on MAS' expectations on how a costs-and-benefits analysis should be incorporated into an institution's risk appetite framework; and

(iii) sub-paragraph (d) – the reference to tolerance for disruption overlaps with concepts that are typically defined within the operational resilience framework. Impact tolerances for disruption to FIs critical business services should be established through the resilience framework, with the TPRM framework ensuring

that third-party arrangements material to the delivery of those services can meet the defined tolerances under severe but plausible scenarios. We take the view that acknowledging this would better align the Guidelines with existing resilience and risk management frameworks and avoid duplication of risk tolerance concepts across different control frameworks.

More generally, FIs should be able to consider their respective obligations and whether the risk appetite and risk management standards of their third-party service providers are not inconsistent with the FI's obligations. Thus, third-party service providers should be able to only meet baseline requirements for areas such as security, resilience and incident response, without FIs having to impose identical KRIs or control frameworks on them as may apply to the FI. We suggest that FIs be permitted to apply similar standards by way of minimum baseline controls and additional risk-based requirements, with allowance for alternative forms of assurance (e.g., SOC reports, ISO certifications, independent audits), especially for large global vendors.

For third-party arrangements that would qualify as non-outsourcing currently, given the proportionality approach, FIs note that they would have the flexibility for governance and approval processes to continue to follow established group frameworks, with local oversight overlay. Given the scale and diversity of such arrangements, applying the same level of approval and oversight as material or other third-party arrangements may be disproportionate to their risk profile mainly where services are delivered across multiple entities and supported by existing group policies, standards and processes. Thus, FIs would, under the proportionality approach, be able to exercise oversight at a portfolio level, including monitoring of key themes such as exceptions, delays and other material issues, with escalation where necessary. This approach ensures alignment and maintains operational practicality.

Q7. MAS seeks comments on the proposed expectations on risk assessment in the Guidelines.

The requirements on the risk assessment broadly align with equivalent provisions in the current Outsourcing Guidelines and international standards. The expectations are also broadly consistent with current practice. We agree that risk assessments should cover both financial and non-financial risks, and should be integrated into the FI's broader risk management and internal control processes.

For third-party arrangements that would qualify as non-outsourcing today, we note that given the proportionality approach, FIs would be allowed to apply their internal definition of materiality and risk assessment frameworks, taking into account the nature, scale and risk profile of such arrangements. Applying the outsourcing criteria to non-outsourcing arrangements may not always be appropriate or risk proportionate.

Q8. MAS seeks comments on the proposed areas of due diligence in the Guidelines.

The due diligence provisions are broadly consistent with the themes reflected in the existing Outsourcing Guidelines and relevant international standards. However, the Guidelines extend these expectations across the wider population of third-party arrangements, and introduce more detailed considerations – including concentration risk and resilience-related factors.

While we acknowledge that proportionality is generally embedded in the framework, given the expanded scope of the Guidelines, requiring extensive due diligence for all third parties may be disproportionate – it is important that the due diligence requirements are calibrated in a way that reflects the level of risk associated with the arrangement.

Thus, we recommend that the framework explicitly distinguishes between baseline due diligence expectations that apply across all third-party arrangements, and enhanced due diligence requirements that are appropriate only for material third-party arrangements and/or material arrangements supporting critical business services. This is particularly relevant for more intensive or resilience-related considerations, such as paragraph 6.8(c)(vi) – benchmarking against recovery or service restoration expectations – which may be appropriate for arrangements that play a material role in supporting critical business services, but would not be proportionate if applied across all third-party arrangements. Alternatively, we strongly recommend that MAS includes an explicit statement at paragraph 6.8 that the due diligence approach should be commensurate with the nature, materiality and risk profile of the third-party arrangement, and that enhanced due diligence measures are expected only where the arrangement is material and/or could have a material impact on the FI's ability to deliver critical business services.

In addition, we respectfully propose that MAS explicitly recognises standardised independent assurance (e.g. ISO certifications, SOC/ISAE reports, and independent assessments) as meeting MAS' expectations – especially where bespoke audits or extensive onsite assessments may not be feasible).

In relation to paragraph 6.9 of the Guidelines, we note that onsite inspections are not required, particularly where equivalent assurance exists, as this would support proportional outcomes. Moreover, onsite inspections may be impracticable as certain service providers do not permit individual client site visits (e.g. because they are themselves regulated).

In relation to paragraph 6.12 of the Guidelines, we note that the considerations largely form an FI's decision-making and procurement process, rather than its due diligence process, which is typically focused on assessing the risk profile of the selected third party. Hence,

we suggest removing these considerations. Should MAS decide to retain them, we suggest carving out these considerations into the risk assessment process in section 6 of the Guidelines instead.

Similarly, paragraph 6.14 of the Guidelines, which addresses the assessment of concentration risk, is more appropriately a component of the risk assessment process, rather than due diligence on the service provider, because concentration risk is an FI-level consideration that relates to aggregate dependencies and substitutability (as assessed during the risk assessment under paragraph 6.3(d) of the Guidelines).

The expectations in paragraph 6.13 of the Guidelines are prescriptive, particularly in relation to specific checks on service provider staff. While we support the objective of ensuring service providers have sufficient and appropriate personnel to deliver services, this level of detail may not be appropriate or feasible across all third-party arrangements. In practice, direct visibility into individual staff performing the services may be limited, and such checks are typically addressed through broader due diligence and control assessments. We recommend this requirement be framed with greater flexibility, so that such checks can be addressed through broader due diligence and control assessments, and the extent of such assessments and checks are subject to the level of risk and materiality of the arrangement. For example, FIs can focus on the service provider's risk management/HR/conduct policies.

Separately, part of the due diligence process includes "disaster recovery arrangements and disaster recovery track record benchmarked to the FI's Service Recovery Time Objective (SRTO) in case of a disruption of a critical business service". FIs note that it would be open to them to benchmark this against their Important Business Services (IBS) and Impact Tolerance (ITOL), which is the maximum tolerable duration of disruption beyond which it could pose tolerable harm, and work with the relevant third parties to recover before the ITOL limit is reached.

Q9. MAS seeks comments on the proposed expectations on contracting in the Guidelines.

We anticipate facing challenges in renegotiating contracts with third-party service providers, as certain critical providers operate on standardised global contracts (e.g. large tech providers).

In relation to paragraph 6.17, the Guidelines appear to place undue emphasis on contractual renewal as the primary means of maintain control. In practice, effective oversight is achieved through a combination of contractual provisions and ongoing monitoring, including periodic assessments and reviews of the third party.

In relation to the provisions that should be included in material third-party arrangements (as set out in paragraph 6.19 of the Guidelines, we have the following comments:

(i) Regarding the expectations surrounding notification of adverse developments in sub-paragraphs (a) and (c), please also refer to our response to Question 16.

(ii) Sub-paragraph (c) – FIs should only be required to report adverse developments that have actual/confirmed impact, as developments that "could impact" the FI is too broad and could result in overreporting of incidents and resource burden to both the FI and MAS. In relation to the notifications provided by an FI, we seek confirmation that MAS will calibrate its expectations, taking into account the reality that (1) a service provider may want to control to whom updates are given, especially during an active incident response, such that an FI may not be able to share everything that the service provider shares with it (apart from general updates); and (2) it is likely to be difficult to require a foreign service provider to cooperate with MAS "in any and all aspects of incident management and investigation" without substantial qualification.

(iii) Sub-paragraph (e)(ii) – global and systemically important service providers may be unwilling to agree to open-ended termination provisions triggered by supervisory direction. Moreover, this requirement could have a significant operational impact on an FI at a group level, where group-level contracts with service providers may need to differentiate jurisdictions where regulators may direct termination of services, and where service providers may be concerned about regulatory risk in a single jurisdiction, potentially triggering global contract termination. (see also our response to Question 16). Hence, we respectfully request that this sub-paragraph be made less prescriptive.

(iv) Sub-paragraph (g) – the expectation to use measurable performance indicators and stipulate the involvement of FIs in periodic testing should not be assumed to apply to all material third-party arrangements (see our response to Question 18). Hence, we recommend flexibility for FIs to determine when these measures are appropriate, based on the level of risk and potential impact of the arrangement (rather than treating them as standard expectations for all material arrangements) and this should be explicitly provided for. For example, where these measures are not appropriate, this sub-paragraph may be satisfied through alternative, risk-based assurance mechanisms such as (1) obtaining periodic independent assurance reports, certifications, or audit reports (e.g. SOC reports or equivalent) covering the service provider's BCP and disaster recovery framework and test outcomes; (2) relying on summary reports or executive attestations from the service provider confirming that BCP and disaster recovery testing has been performed, including key findings and remediation actions, without requiring FI participation in the testing itself; or (3) aligning measurable indicators (such as recovery time objectives) to the nature of the service provided and the FI's dependency on that service, rather than adopting a uniform standard.

(v) Sub-paragraph (i) – while contractual remediation linked to regulatory requirements is generally understood, extending this expectation to supervisory requirements goes further, and it is unclear whether this refers to formal supervisory instruments that imposes specific obligations, or (more broadly) to supervisory views, feedback or inspections during the course of supervision. If the latter (and interpreted broadly), this expectation could result in repeated contractual remediation, which may not be achievable in practice. We therefore recommend removing the reference to "supervisory" requirements, or clarifying the circumstances in which this would justify contractual modification. We also note that, in practice, service providers may require evidence of the "supervisory requirements" before agreeing to contractual modifications. Where such requirements may be based on supervisory feedback (if this is what MAS intends), inspections or broader supervisory communications between MAS and the FI, this information is typically confidential and not capable of being shared with third parties. This further underscores that extending contractual remediation to "supervisory requirements" is not workable in practice.

(vi) Sub-paragraph (l) – specifying all locations where data is processed and stored may also conflict with the operational model of cloud and SaaS providers whose infrastructure is designed for dynamic workload distribution, and make it challenging to negotiate such a contractual requirement. Hence, we suggest express confirmation that this requirement may be implemented proportionately.

In terms of alignment with MAS Notice 658, we propose that paragraph 6.19 of the Guidelines be amended to replicate the existing required contractual provisions set out in MAS Notice 658, rather than introducing an enhanced set of contractual provisions. Certain bank members may have dedicated resources to negotiate and update their contracts with multiple internal and external service providers to comply with the requirements in MAS Notice 658. It is anticipated that further renegotiations for these same contracts with the service providers (particularly external providers) in order to incorporate an enhanced set of contractual provisions would face challenges.

In relation to paragraph 6.22 of the Guidelines, we propose that MAS allows flexibility by not prescribing specific approvers such as the second line of defence or senior management. A risk-based approach should permit FIs to determine the appropriate reviewer, including delegation to an authorised committee and the use of established group-level processes, as long as Singapore-specific risks are addressed. This avoids duplicative approvals while maintaining effective oversight.

In relation to paragraph 6.39 of the Guidelines which deals with the return or destruction of data on termination, we note that large international service providers often need to keep information post termination where required by regulation (as opposed to laws), and

suggest that this should be acceptable as long as the information is kept confidential and in an offline environment.

Q10. MAS seeks comments on the proposed expectations on onboarding and ongoing monitoring, particularly in relation to the frequency of due diligence and audit. FIs which prefer more explicit guidance on the appropriate timeline/frequency of due diligence for material third-party arrangements should indicate their view on an appropriate frequency and the reason for the FI's proposed frequency.

General comments relating to section 6 of the Guidelines

FIs engage a variety of third-party services, some of which are performed onsite under the FI's internal controls and direct supervision. In such cases, FIs may consider the extent to which compliance with certain requirements applies, such as audit or business continuity plan testing, so long as baseline vendor due diligence is proportionate to residual risks. For such services, we highlight that certain parts of the Register may be left blank (e.g. column AB "When was an independent audit last conducted on the service provider / material sub-contractor?").

In addition, we suggest having a more streamlined onboarding and offboarding approach where an existing third-party service provider provides additional services. This would allow FIs to focus risk assessment at the level of the third-party service provider, rather than repeating due diligence at the level of the third-party arrangement, where there may be significant overlap and synergies.

The Guidelines delineate risk assessment and due diligence as distinct sections, processes, or steps to be undertaken prior to contracting or periodically when significant changes occur. We respectfully submit that information procured on a third party during the due diligence stage complements the FI's risk assessment on a particular third party. Thus, whilst the due diligence section is separate from the risk assessment section, the processes may be interlinked and complementary in relation to the risk assessment of a particular third-party service provider.

Frequency of due diligence and audit

We are supportive of MAS' approach to allow firms flexibility to determine the frequency of due diligence and audit on a risk-based basis, rather than prescribe fixed timelines or frequencies. This is consistent with international standards and regulatory approaches which require firms to determine the nature, frequency and intensity of due diligence proportionate to the risk and materiality of the arrangement. We do not consider it appropriate to introduce explicit guidance or prescriptive expectations on frequency, as this would undermine the risk-based and proportionate approach. Frequency should remain a risk-based determination for firms, supported by internal risk management frameworks and proportionate principles.

However, we respectfully request that the frequency of audit should not be specified as requiring board approval in every case (as currently required under paragraph 6.30 of the Guidelines) and this can be left to FIs to determine.

Onboarding and ongoing monitoring

While we support the objective of ensuring that ongoing monitoring remains risk-based, the current drafting introduces ambiguity as to how FIs should determine the appropriate level of oversight. In particular, the reference to scaling monitoring to the materiality and complexity of (inter)dependencies (at paragraph 6.27 of the Guidelines) does not provide a clear basis for calibrating monitoring expectations. We are of the view that, in practice, the level of ongoing monitoring should be driven primarily by the risk profile and materiality of the arrangement. We therefore recommend that paragraph 6.23 of Guidelines explicitly state that the nature, frequency, and intensity of ongoing monitoring should be determined by and commensurate with the nature, scope and materiality of the arrangement, the nature and extent of risk, and the potential impact of a failure or disruption.

Separately, we note that MAS expects FIs to monitor regulatory developments affecting third-party arrangements and to assess the impact of material changes. In practice, FIs may face challenges in continuously tracking and interpreting regulatory changes across all jurisdictions where service providers operate. Hence, we suggest that MAS expressly states that FIs will be able to adopt a risk-based, proportionate approach for this requirement.

In relation to paragraph 6.23 of the Guidelines, the current drafting requiring an FI to ensure that the third-party service provider has adequate understanding of the FI's policies, people, processes, technology, facilities and interconnections that are needed to provide the service, may be unduly burdensome for the FI. It may not be feasible at the onboarding stage for the FI to inform the third-party service provider of such information with a view to ensuring that the service provider has adequate understanding. In practice, the FI would pose directed questions to the third-party service provider as part of its onboarding and due diligence process which relate to the third-party service provider's policies, people, processes and technologies which are relevant for the provision of the service.

In addition, we are proposing that the expectation under 3.6 of the Consultation Paper (6.23 of the Guidelines) for FIs to map dependencies and interconnections relating to its material third-party arrangements be restricted to material third-party arrangements supporting critical business services, to align with the requirements set out under MAS Guidelines on Business Continuity Management. Expanding this requirement to all material third party arrangements may create significant operational burden to financial institutions.

Third-party management group

In relation to paragraph 6.28(b) of the Guidelines, which states that third-party management group(s) should comprise members from different risk and internal control functions (e.g. legal, compliance, IT risk management and finance), we recommend that MAS explicitly acknowledges that this may be viewed as an illustrative example of good practice, with flexibility for FIs to adopt alternative governance structures that achieve similar outcomes, thereby allowing firms to reflect existing governance arrangements and ensuring alignment with proportionality principles.

Separately, we seek clarification on the expectation in paragraph 6.28(f) of the Guidelines, which requires periodic reviews by the second or third lines of defence on all material third-party arrangements to ensure that the FI's third-party risk management policies, standards and procedures, and these Guidelines, are effectively implemented. For some members, internal control functions (second line of defence) may be part of the third-party management control group to be established as part of paragraph 6.28(b) of the Guidelines, and where FIs are subject to periodic audits covering governance and third-party risk management, we propose that FIs can, depending on their internal operational model, comply with paragraph 6.28(f) of the Guidelines by engaging a qualified party who possesses the expertise to perform the review, and is independent of the entire outsourcing review /monitoring processes.

In relation to paragraph 6.28 of the Guidelines, for clarity, we suggest that MAS expressly states that board approval is at the classification level, i.e. due diligence should relate to material third-party arrangements (as a whole) and not for each specific material third-party arrangement.

Independent audit

We support MAS' proposal to focus the independent audit scope on material third-party arrangements. We respectfully request that MAS further differentiates the independent audit requirements between external third-party arrangements and intragroup relationships, given the increased control and influence exercised over providers within the same group. This includes considerations such as shared governance structures, internal audit systems and risk management frameworks. The differentiation for intragroup relationships may also be allowing FIs to rely on the periodic due diligence done on the material arrangements to meet the audit requirements. This allows for FIs to focus the independent audit of material external third parties.

Q11. MAS seeks comments on the proposed expectations on termination.

We note that the termination and exit requirements are detailed and do not distinguish between expectations that apply to material and non-material arrangements, or between planned termination scenarios and unplanned exits. The Guidelines link the level of detail of exit plans to the materiality of the arrangement; however, a greater level of detail does

not necessarily make exit plans more effective, and this may not represent the most appropriate risk-based approach in practice. Moreover, the cost to maintain and test exit plans may be disproportionate if such requirements apply to all third-party arrangements (or, if they only apply to material third-party arrangements, but materiality is too broadly defined). Further, effective exit management should not become a paper-driven or compliance-led exercise. In practice, the ability to execute exit strategies or plans depends on a range of measures, with exit planning supported and underpinned by contractual safeguards, substitutability assessments, ongoing monitoring and established group-level resilience frameworks. We therefore encourage an outcomes-focused approach that centres on the FI's ability to execute an orderly exit when required, rather than prescriptive documentation of specific termination scenarios in all cases.

We also recommend applying exit planning and testing expectations on a risk-based and proportionate basis, with the requirement being explicitly limited to material third-party arrangements that could have a material operational, customer or prudential impact, rather than requiring the same level of planning and testing across all third-party arrangements.

We also suggest that MAS explicitly acknowledges that exit plans may include phased exit strategies, interim risk mitigants and "exit-to-alternate" vs "exit-to-internal" considerations, and not necessarily involve immediate termination – this is because for certain services (cloud, core platforms, utilities), exits may be multi-year and constrained by interoperability and market options. In addition, FIs may adopt practical safeguards such as linking final payments to the fulfilment of exit obligations.

Intragroup arrangements

We suggest that MAS explicitly acknowledges that FIs may comply with the expectations on termination for intragroup arrangements using a proportionate approach. This is because termination may not always be operationally feasible for certain critical intragroup or infrastructure services. In such cases, alternative mitigating measures (e.g. contingency plans, manual workarounds, enhanced monitoring, intragroup escalation) may be more appropriate than termination. This would help ensure alignment between contractual expectations and practical constraints, particularly for systems managed at the head office level.

Unplanned termination

Both planned and unplanned terminations can, in practice, involve complex migration exercises, which may require extended time to execute in a safe and secure manner, and do not typically offer the immediacy required for business continuity solutions deployable within hours or days. We therefore encourage MAS to ensure that expectations around unplanned termination appropriately reflect operational realities, including the time required to transition services. While mitigation options may be available, they may not be

feasible or proportionate in all cases. In particular, maintaining standby vendors or in-house solutions may introduce significant cost and operational burdens, and ultimately be unfeasible in practice, and should not therefore be assumed as a baseline expectation for business continuity measures.

Q12. MAS seeks comments on the scenarios under which an FI should consider whether to terminate the service provider agreement for a third-party arrangement and the circumstances under which MAS may direct an FI to terminate the agreement.

In relation to paragraph 6.36 of the Guidelines, which sets out the circumstances when an FI should consider terminating the service provider agreement, we note that termination scenarios are framed broadly, and it could be challenging to reflect such a wide range of circumstances contractually. In particular, we note that sub-paragraphs (c), (f) and (g) extend beyond situations where the service can no longer be performed and include broader circumstances that would not automatically justify termination without taking into account the severity or the potential impact to the FI. We suggest that these provisions should be applied through a risk or impact-based lens, and the Guidelines should specify that termination should only be considered where the circumstances will have a material adverse impact.

In relation to circumstances which MAS may direct termination, the power for MAS to direct termination is broad. Particularly, we note that under paragraph 6.37(g) of the Guidelines, MAS may direct termination where MAS is prevented from obtaining information. However, in some scenarios, termination may not be the most suitable course of action. For example, in the context of non-Singapore service providers, such providers may find it difficult to cooperate with MAS requirements (e.g. they may have legitimate legal reasons such as data protection laws, blocking statutes, or legal privilege for limiting disclosure to a foreign regulator). Moreover, termination may have severe operational consequences for a large global FI, especially with global service providers (see also our response to Question 16). Further, in practice, many FIs, especially subsidiaries of global financial groups, rely on service providers that are contracted by an affiliated or parent entity, rather than by the local FI itself. In such cases, the local FI may not have unilateral contractual authority to terminate or not renew the arrangement, notwithstanding its best efforts to manage and mitigate the attendant risks. This structural limitation may apply even where the FI has otherwise demonstrated appropriate governance, oversight, and risk management over the service. MAS should instead exercise supervision by requiring an FI to demonstrate that it has taken reasonable and timely steps, on a best-efforts and risk-proportionate basis, to remediate and mitigate risks.

Should MAS decide to retain its right to direct termination, we note that paragraph 6.38 of the Guidelines provides that MAS will "endeavour" to give reasonable notice of its intention to direct termination. However, given the potential operational and customer impacts, this

threshold could be strengthened to explicitly provide for sufficient notice and appropriate engagement with the FI ahead of any such direction, to enable MAS to fully understand the consequences and assess whether termination is the most appropriate cause of action. Where termination is not practicable in the short term or is not the most proportionate or practical risk mitigant, the Guidelines should explicitly provide that MAS will consider interim risk mitigation and transition measures (e.g. additional controls, reduced scope, migration roadmap, group-level escalation mechanisms). Further, any direction to terminate should be based on the severity of risk (including systemic impact), taking into account feasibility and potential consequences of termination; more generally, MAS may expressly set out criteria that it would consider before directing termination.

In relation to paragraphs 6.37(e) and (g) of the Guidelines, we highlight the challenges that FIs may face in incorporating the audit right clauses without limitations (as mentioned in our response to Question 9).

Q13. MAS seeks comments on the proposed expectation for FIs to ensure the service provider notifies the FI in writing prior to the engagement of a material sub-contractor, where possible. Feedback on the inclusion of material sub-contractors in the register of third-party arrangements should be provided in Question 3.

This expectation (strictly applied) may be difficult or impracticable to meet in certain circumstances. Particularly, for large, global service providers, where sub-contractors may be engaged dynamically (e.g. for technology, infrastructure, or specialist services), sub-contractor engagements may occur outside the FI's direct visibility or prior knowledge – especially where the FI relies on group-wide or multi-jurisdictional arrangements, and where local contractual control is limited. In addition, the global service providers – especially those operating outside Singapore – may not themselves be subject to uniform regulatory requirements to conduct prescriptive due diligence on their sub-contractors. As a result, a strict prior-notification requirement would not be feasible, notwithstanding the FI's reasonable efforts.

We appreciate MAS' acknowledgement of the inherent limitations arising from the fact that FIs do not have a direct contractual relationship with subcontractors. As recognised by MAS in paragraph 3.32 of the Consultation Paper, FIs manage supply chain risk through their direct relationship with the appointed service provider, typically through contractual arrangements that require the service provider to cascade relevant risk management and control obligations to material sub-contractors.

However, the footnote to paragraph 7.2(a) risks implying that FIs are expected to take reasonable steps directly in respect of sub-contractors. We suggest clarifying that "reasonable steps" are taken only through the FI's direct relationship with the service provider, and not through sub-contractors:

[61] *Where an FI allows a service provider* ~~***or sub-contractor***~~ *to determine whether a new sub-contracting arrangement is material and warrants notifying the FI, the FI should take reasonable steps to ensure the service provider* ~~***or sub-contractor, as the case may be,***~~ *has a robust process to do so.*

More specifically, we respectfully note that FIs can achieve this through a combination of contractual safeguards and ongoing assurance mechanisms, such as:

(i) requiring service providers to provide periodic attestations confirming that appropriate due diligence and risk assessments are performed when onboarding material sub-contractors; and

(ii) incorporating contractual provisions requiring service providers to notify the FI of any material adverse developments involving sub-contractors, including incidents, control failures, or significant changes that may impact the FI.

Q14. MAS seeks comments on the proposed guidance on pass through sub-contracting.

We respectfully request that paragraph 7.3 of the Guidelines should not apply to pass through sub-contracting arrangements to intragroup service providers (i.e. where the FI's head office or branches act as the service provider). In practice it may not be feasible or necessary for paragraph 7.3 to apply to intragroup service providers, as oversight of sub-contracting is undertaken by an FI's intragroup service provider. In such circumstances, the extent of "effective oversight" by an FI would be more limited and should be interpreted accordingly. We also seek clarification on whether the pass through requirements apply to 4th party sub-contractors and beyond.

Q15. MAS seeks comments on the proposed expectation that an FI should take reasonable steps, on a risk proportionate and best effort basis, to ensure that material sub-contractors are held to similar standards as service providers.

We appreciate that the expectation to ensure that material sub-contractors are held to similar standards as service providers is on a risk-based, proportionate, and best effort basis. In practice, this is typically achieved through the cascading of contractual obligations from the FI to the third-party service provider, with the third-party service provider responsible for imposing equivalent requirements on its sub-contractors. This reflects established market practice and appropriately recognises that the FI does not have a direct contractual relationship with sub-contractors. With such a practice, it would also be challenging and operationally burdensome for FIs to obtain the relevant information needed to hold material sub-contractors to similar standards as service providers (e.g. obtaining information relating to the risk and control frameworks of sub-contractors), and to enforce standards. In addition, where sub-contracting arrangements are already established by the service provider prior to the FI's engagement and are embedded within the service provider's operating or delivery model, the FI's ability to influence

sub-contractor standards is necessarily indirect and dependent on the service provider's own governance and risk management framework. Hence, a risk-based, proportionate approach would be essential to fulfilling this expectation. Similar to our response to question 13 of this Consultation Paper, we therefore suggest that MAS considers recognising alternative, risk-based means for FIs to meet this expectation, such as reliance on contractual undertakings from service providers or periodic attestations over the service provider's oversight of its material sub-contractors, particularly for arrangements assessed to be higher risk or critical.

To more accurately reflect the risk-based, proportionate and best effort basis, we propose the following amendment to paragraph 7.1 of the Guidelines:

> *7.1 The expectations in the Guidelines on FIs' management of risks from service providers in material third-party arrangements should* ~~***be read to extend to FIs' management of risks from material sub-contractors in such arrangements,***~~ *where possible****, be applied by the FI through its contractual arrangements with the service provider to ensure that relevant risk management and oversight obligations are appropriately cascaded to material subcontractors.***

In addition, the current draft in paragraph 7.5 of the Guidelines risks being interpreted as more prescriptive, as it might imply that FIs are expected to ensure or verify that specific provisions are included within sub-contracting arrangements to which they are not a party. We therefore suggest paragraph 7.5 be reframed as follows:

> *7.5 For material third-party arrangements, an FI should take reasonable steps, on a risk proportionate and best effort basis, to ensure that* ***the third-party service provider holds*** *material sub-contractors* ~~***are held***~~ *to similar standards as service providers. This could be through the inclusion of appropriate provisions in its agreement with service providers. An FI should endeavour to ensure the following* ***in relation to material sub-contracting arrangements****:*
>
> *[…]*
>
> *(b) that* ***the FIs agreement with the service provider includes provisions requiring the service provider to ensure that the*** *sub-contracting agreement* ***to a material sub-contractor*** *includes the following provisions: …*

The above amendments will help ensure that the expectation set out at paragraph 7.5(a) of the Guidelines will not require (and should not require) an FI to directly notify sub-contractors in writing of confidentiality obligations under relevant legislation and common law. This requirement would be burdensome and not practical. As noted, in practice, FIs incorporate sub-contracting provisions within service provider agreements to safeguard

the confidentiality and integrity of all information under their custody. More generally, it should be made clearer in the drafting that paragraph 7.5 of the Guidelines only applies to material third-party arrangements.

Q16. MAS seeks comments on the proposed expectation of FIs and service providers in relation to adverse developments.

In relation to paragraph 8.1 of the Guidelines, we seek clarification on –

(i) the definition of "adverse development";
(ii) timing (including incident notification timelines);
(iii) how information should flow from third parties (and the expectation where service providers are constrained by legal privilege, cross-border disclosure limits or contractual limitations, and allow staged disclosure and validated summaries); and
(iv) the scope (including whether risk-based updates to MAS are allowed).

In relation to reporting requirements set out in paragraph 8.1 of the Guidelines, we suggest that the requirement for MAS to be informed in the case of an adverse development should not be a separate regime from the MAS Notice on Technology Risk Management and the impact should align with "relevant incident" under that framework – i.e. if a third party causes an "adverse development" that does not amount to a "relevant incident", then the FI should not be required to report it to MAS. Additionally, we take the view that FIs should only have to report adverse developments with actual/confirmed impact that reaches the reporting thresholds based on existing MAS regulations, and not "any event that could lead" to an impact on the FI.

In relation to paragraph 8.2, we note that FIs do not have absolute control over their service providers and cannot guarantee their level of cooperation (even if FIs formally request that service providers cooperate with MAS). This expectation may also encourage an uncoordinated approach to obtaining information from a third party, and they may be inundated with information requests, some of which they are unable to fulfil by law. Overall, should further information be required on service providers in such circumstances, instead of requiring the FI to terminate its arrangements with the service provider, it is respectfully requested that MAS could request the information directly from the service provider in the first instance. The proposed broad powers for MAS to request termination in egregious cases where cooperation from service provider is lacking (as per paragraph 8.3 of the Guidelines) could have far reaching implications, especially if there is no feasible alternative (whether one does not exist or the alternative is less mature in security or resilience), or if there is no realistic ability to move to another third party. Moreover, many FIs may rely on service providers engaged under group-wide or regional contracts. In such cases, the local FI may in practice be less able to terminate the services of a service provider engaged at the group level, even where it exercises robust local oversight and escalation. Hence, we respectfully request that MAS does not adopt requirements that are akin to prescription of which service providers an FI should use (as it should be a risk-based

decision). Should MAS retain this power, MAS should not be able to make this decision unilaterally; it must be done in conjunction with the FI.

On a separate note, we would also respectfully request that MAS should gather FI-related information directly from FIs, not from service providers, and also request only service provider information or general sectoral information from service providers, not information specific to an FI in breach of confidentiality clauses between FIs and service providers.

Reporting requirements for global FIs

Global FIs may have to manage reporting and responding to multiple regulators in an adverse development. In addition, there may be different (and possibly conflicting) legal obligations on the FI. Hence, we seek MAS' assurance that its expectations on timing and information provision would be calibrated accordingly, including allowing for reasonable flexibility where FIs are required to coordinate responses across multiple regulatory authorities.

Separately, for intragroup arrangements and third-party service providers supporting critical systems, the local FI may face challenges in obtaining timely and complete information, as the systems may be managed outside the local FI and the local FI may not have direct control over the service provider's incident investigation or reporting processes. Hence, we propose that MAS clarifies that FIs may rely on service provider reporting and escalation frameworks, including intragroup arrangements, to fulfil the expectations set out in section 8 of the Guidelines. Nonetheless, we note that FIs will need to ensure that appropriate escalation channels are established with service providers, and sufficient minimum information (e.g. nature of incident, impact, remediation actions) can be obtained within a timeframe that supports regulatory notification obligations.

Q17. MAS seeks comments on the list of "exempted services". Where there are any additional categories of services that may require exemption, respondents should provide the rationale to support their suggestion for these services to be exempted.

We seek further illustrative examples of services that would and would not fall under paragraph 1(c) of Annex 3 of the Guidelines.

We suggest that the following categories of services should be exempted, and if they are not, we suggest that they should be subject to reduced due diligence:

(i) Market information services such as those provided by Bloomberg, MSCI, Moody's and Standard & Poor's, because these services:
   (a) provide standardised, non-customised information;
   (b) do not process or store the FI's proprietary customer data or systems; and
   (c) do not create operational dependency on regulated activities.

(ii) Services provided by professional associations such as The Association of Banks in Singapore (ABS), Singapore Business Federation (SBF), ASFIMA and Investment Management Association of Singapore (IMAS), because these associations operate

as industry advocates and standard setters rather than third-party service providers.

(iii) Services that are excluded services under Annex B of MAS Notice 658 – should MAS decide not to exclude those services, we respectfully request that MAS minimally exempt the following because they are either provided by professional firms regulated in their respective industries, or are provided within the bank's premises/environment and do not pose significant risk from a third-party angle:

(a) brokers, dealers and brokerage firms;

(b) correspondent custody & clearing banks (CCCBs) and correspondent banking services, including (i) the maintenance of custody accounts with specified custodians as required under Regulation 27 of the Securities and Futures (Licensing and Conduct of Business) Regulations; and (ii) clearing and settlement arrangements between clearinghouses and settlement institutions and their members, and similar arrangements between members and non-members;

(c) entities providing insurance services and product distribution;

(d) entities providing alternative products and investment solutions;

(e) government agencies;

(f) consulting / advisory / expert opinion services (e.g. Big 4, Legal firms);

(h) bill payment services;

(i) supply and maintenance of emergency and incident-response equipment;

(j) training on usage and technical support of third-party IT tools;

(k) resource augmentation provided by professional firms (e.g. IT firms) where such services are performed within the bank's premises and subject to the bank's oversight;

(l) partnership and sponsorships;

(m) international payment networks such as MasterCard and Visa.

(n) telecommunication services and public utilities (e.g. electricity, SMS gateway services);

(o) postal services;

(p) introducer arrangements and principal-agent distribution arrangements where the financial institution does not have any contractual relationship with underlying customers/investors and the intermediary is responsible for customer due diligence and safeguarding customer information; and

(q) statutory audit and independent audit assessments.

(iv) Payment systems and payment schemes subject to regulatory oversight, including domestic schemes (e.g. those supervised by the Singapore Payment Network) and international payment networks (as above).

(v) Regulated exchanges and trading venues that are not technically "Financial Markets Infrastructures".

(vi) Government-mandated services provided by regulators, Government-appointed organisations or quasi-governmental bodies inside or outside of Singapore.

(vii) Ancillary services provided by SWIFT, which may be material to some FIs.

(viii) Staff augmentation and recruitment agency services (FIs engage with multiple recruitment agencies for commercial reasons, and it would be burdensome to update the Register for these services on an ongoing basis).

(ix) Business transformation and change management.

(x) Travel and transportation.

(xi) Facility management and building operations.

(xii) Professional and business services.

(xiii) Financial and administrative services.

(xv) Employee services.

(xvi) Purchases/subscriptions of published information such as one-off reports or books and hardcopy or electronic subscriptions to trade/research journals, reports and magazines. These services, though beneficial knowledge for the FI's business, are one-way information sharing to FIs where there is no confidential data shared.

(xvii) low-value arrangements (based on the FI's internal thresholds) – these arrangements typically present lower risk and are managed with proportionate governance and controls; applying the full set of requirements under the Guidelines could result in disproportionate operational effort.

(xviii) Third Party Platform (TPP) services, which function as bank-neutral, multi-bank cloud-based (SaaS) trade platforms due to the following:

(a) no functions or infrastructure owned by the bank are delegated or outsourced to the TPP. TPPs do not conduct credit decisioning, document examination, compliance reviews, nor do they serve as a record maintaining system for the bank's trade transactions.

(b) for banks and clients, there is no operational reliance on TPPs. In the event of TPP unavailability, corporate clients can very easily utilize the bank's existing digital channels or transact over the counter, ensuring continuity of core documentary trade services and adherence to regulatory requirements.

(c) banks retain full control and end-to-end accountability for back office transaction processing, decision-making and risk management. Existing operational checks and controls for banks remain unchanged.

(xix) Arrangements that pertain to principal-agent relationships, such as the engagement of distributors to distribute collective investment schemes.

<u>Requirements relating to exempted services</u>

We support the implementation of risk-proportionate and appropriate business continuity measures, as well as incident response plans, to address the risks associated with the use of exempted services.

However, we note that this may not be feasible for certain services, such as Financial Market Infrastructures and systemically important payment systems. Thus, we respectfully request that MAS provides greater flexibility regarding this requirement, either by including the phrase "where feasible" or by establishing a separate requirement for Financial Market Infrastructures and systemically important payment systems, distinct from other services such as cleaning, gardening, or pantry operations.

Q18. MAS seeks comments on other aspects of the Guidelines that have not been covered in earlier questions.

Concentration risks

We respectfully suggest that concentration risk management should remain risk-based (as per an FI's risk appetite and risk threshold) – while concentration risk is one of several factors considered, it should not, in isolation, disqualify an otherwise suitable service provider, as such risks are assessed holistically and mitigated through appropriate controls and oversight.

We note that the proposed mitigation measures in paragraph 6.14 of the Guidelines are prescriptive and risk being interpreted as de facto minimum requirements for managing concentration risk. Applying these mitigation measures across the full population of third-party arrangements would not be proportionate and we encourage a pragmatic and risk-based approach to concentration risk which, we note, is not inherently bad. That is, the objective should not be to eliminate concentration, but to ensure that it is appropriately identified, assessed and managed where it creates a meaningful exposure.

Effective concentration risk management may focus on identifying areas of dependency, assessing the potential impact, and determining whether mitigation is necessary and proportionate considering the level or risk and the measures that are available. In particular, the following expectations may not be in all cases operationally or technically feasible, or reasonable to implement for all arrangements:

(a) enhanced monitoring;
(b) more frequent business continuity and disaster recovery plans;
(c) combining FI on-premises infrastructure with third-party services' – this would typically be deployed for security purposes and is not necessarily an appropriate measure for addressing concentration risk;
(d) having alternative providers with minimal downtime; and
(e) retaining capability in-house.

The Guidelines should therefore specify that the mitigation measures listed in paragraph 6.14 of the Guidelines are illustrative, rather than mandatory, and should not be treated as minimum expectations applicable in all cases. Mitigation actions should be determined

based on the nature of the arrangement, the degree of dependency, and the FI's ability to influence or reduce the risk.

In addition, we suggest that MAS gives distinct consideration to significant or systemic third parties and monopolies in relation to concentration risk. In practice, many third-party services relied upon by FIs – such as fund administration, custody, market infrastructure, and certain technology services (e.g. cloud service providers) – are provided by a small number of large, reputable, and systemically important service providers. These markets are, by nature, highly concentrated, and the availability of viable substitutes is often limited. As a result, the ability of FIs to meaningfully reduce concentration risk through diversification may be constrained, notwithstanding reasonable risk management efforts. Hence, we propose that the Guidelines explicitly recognise that reliance on one or a small number of global, well-established service providers does not, in of itself, indicate inadequate concentration risk management, provided the FI can demonstrate that:

(i) the reliance is deliberate, risk-assessed, and consistent with the FI's risk appetite; and

(ii) the risks arising from such concentration are actively monitored and subject to appropriate governance and escalation.

<u>BCP</u>

We welcome the explicit acknowledgement of a risk-based approach in paragraph 10.3, which states that business continuity measures should be commensurate with the nature, scope and complexity of the arrangement. We recommend that this be expanded to also refer explicitly to the level of risk and the potential impact of the arrangement. Given the scope expansion, the Guidelines should make clear that the BCM and disaster recovery requirements are applied in a risk-based manner, with more extensive measures (e.g. testing) expected only where an arrangement presents a higher level of risk or potential impact.

Specifically, the expectations in paragraph 10.4 regarding reciprocal BCM and disaster recovery testing should be limited to material third-party arrangements that are material to the delivery of a critical business service. Additionally, there should be explicit flexibility so that participation in testing can be determined on a risk-based approach and where feasible. This would reflect MAS' acknowledgement that involving a service provider in testing is not always applicable and that FIs could, rather than should, take part in service providers' tests. Requiring otherwise would be operationally challenging. This is because:

(1) many service providers, particularly those that are not themselves regulated FIs, are not subject to regulatory requirements to conduct BCP or disaster recovery testing at a prescribed level of rigor or frequency – hence, mandating specific testing standards or measurable indicators comparable to those imposed on FIs may not be feasible or proportionate, notwithstanding their overall operational robustness; and

(2) direct involvement of FIs in service providers' BCP and disaster recovery testing is generally not a common market practice, especially among large global or multi-tenant service providers. These providers often conduct testing at an enterprise or platform level across multiple clients, and operational constraints, confidentiality considerations, and scale limitations may make FI-specific participation impractical.

Similarly, the expectation in paragraph 10.5 to consider severe but plausible scenarios should be amended to reference 'potential' rather than 'set' scenarios and should be applied depending on the nature, scope, complexity, level of risk and impact of the relevant arrangement.

We also recommend that the Guidelines recognise that certain contingency measures – including insourcing or substitution to an alternative provider – may not always be achievable in practice, and should allow FIs to adopt alternative risk mitigation measures where appropriate.

Client Confidentiality and Consent Requirements

We note practical challenges in obtaining client consent for the sharing of confidential information with service providers and their sub-contractors, particularly where standard industry agreements (e.g. ISDA,GMRA,APLMA,LMA) do not include such provisions and are not easily amendable. This is further complicated in scenarios involving secondary market transactions where the FIs may have limited ability to influence contractual terms. In this regard, we would like to seek MAS's clarification whether alternative approaches may be permitted, such as reliance on existing confidentiality undertakings or regulatory safeguards in place of obtaining explicit client consent.

Cloud – Annex 4

We appreciate that this language directly references MAS's 2021 guidance – "Advisory on Addressing the Technology and Cybersecurity Risk Associated with Public Cloud Adoption" – however, we would like to recommend that MAS does not suggest (or lightly prescribe) any specific resilience solutions (e.g. portability, interoperability) to mitigate the risks of vendor lock-in or concentration. Instead, MAS might recommend that FIs take into consideration the risks of vendor lock-in or concentration and that FIs may implement resilience solutions to mitigate that risk, where appropriate. Resilience solutions should not be prescribed so that FIs can make risk-based decisions on how best to mitigate the risks of vendor lock-in or concentration. Additionally, if MAS decides to maintain this language, we request that MAS clarifies that this is suggestive language and not meant to be interpreted by examiners as prescriptive.

More generally, we note that the guidance on cloud services in Annex 4 of the Guidelines is relatively brief and does not address emerging models such as multi-cloud, edge

computing or AI-as-a-Service; multi-tenancy and dynamic data residency challenges are acknowledged but not resolved.

In addition, while we appreciate the inclusion of guidance on cloud computing services within the Guidelines, we propose that MAS considers streamlining the Guidelines by distinguishing between technological considerations and TPRM aspects. For instance, it may be appropriate to address technological topics—such as multi-tenancy, data commingling and physical or logical controls for data segregation—in the Guidelines on Risk Management Practices – Technology Risk. Such an approach would ensure the Guidelines maintains its focus on third-party risk topics.

Q19. MAS seeks comments on the proposed transition period of 6 months.

The proposed implementation timeline of 6 months is not sufficient given the broader scope of the new framework and the number of arrangements that will need to be assessed against the revised requirements. In practice, implementation will require FIs to apply the lifecycle expectations – which are comprehensive – to a much wider third-party population.

We strongly urge MAS to provide a longer and more proportionate transitional arrangement to ensure implementation remains feasible. We recommend:

(a) a transitional period of 24 months. For contracting requirements, we recommend that MAS allows for updates to occur organically through renewal and renegotiation cycles, supported by interim risk mitigations (e.g. documented exception handling, compensating controls, enhanced monitoring) for material arrangements where immediate contractual changes are not achievable (e.g. due to the timing of renewal cycles/ vendor leverage), rather than prescribing a fixed timeframe for contractual remediation; or

(b) a phased implementation approach that distinguishes between material third-party arrangements and non-material third-party arrangements: For material third-party arrangements, FIs would be expected to remediate and align with the Guidelines within the transition period of 24 months, with the initial register submission aligned to this timeframe. This reflects the higher risk and priority associated with such arrangements. For non-material arrangements, FIs would be permitted to address these arrangements at the point of contract renewal (and supported by interim risk mitigations where necessary – e.g. documented exception handling, compensating controls, enhanced monitoring. Where arrangements are evergreen, or do not have defined contracting events, FIs should apply a risk-based approach to ensure remediation within a reasonable timeframe; or

(c) a phased implementation approach that distinguishes between (i) compliance with governance and risk assessment obligations and (ii) compliance with contracting and register obligations – with more time provided for the latter. This would allow

FIs to prioritise and sequence their implementation efforts in a structured and risk-proportionate manner, consistent with the objectives of the Guidelines.

These approaches would support effective implementation, while ensuring that remediation efforts are prioritised towards arrangements that pose the greatest operational and resilience risk.

Drawing from past experience in the implementation of MAS Notice 658, this is because it may take more time to:

(i) assess the revised requirements;

(ii) review and update all relevant policies, procedures and risk assessments;

(iii) obtain approval for uplifting standard contracting templates and contractual provisions;

(iv) renegotiate numerous existing contracts with external third parties (and cascading obligations that relate to sub-contractors). This would take time because some service providers may not be willing to completely comply with the contracting requirements, thus negotiations may be prolonged. In particular, based on past experience, negotiations on audit rights clauses have proven challenging, especially with service providers that are large multinational corporations. For example, FIs have encountered requests from service providers to obligate MAS to certain requirements in the performance of such audits in view of the potential operational burden on them, which is not something that banks are able to accede to on behalf of MAS. In such cases, it may be necessary for FIs to negotiate for a clause that is mutually acceptable. In addition, some service providers may request for higher fees to cater to audit rights clauses. Further, we foresee service providers pushing back on the need to furnish their internal policies, as implied under paragraph 6.19(a) of the Guidelines;

(v) implement the required governance uplift and operating model changes; and

(vi) gather the requisite data to populate the Register (particularly for mid-sized FIs); especially since the revised requirements apply to all third-party arrangements (which may be significantly larger in scope as compared to outsourcing arrangements).