



Banking Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117

29 Jan 2021

Re: Consultation Paper P011-2020 on Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services

To Whom It May Concern,

Amazon Web Services (AWS), one of the leading providers of cloud services to banks in Singapore, sincerely thanks the Monetary Authority of Singapore (MAS) for the opportunity to provide inputs on the *Consultation Paper on Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services*. We understand that this consultation paper follows the 2019 consultation paper on outsourced services and the Banking (Amendment) Act 2020, and intends to set out requirements for (1) ongoing outsourced relevant services of banks, with a focus on material services; and (2) outsourced relevant services involving the disclosure of customer information by banks to service providers.

We appreciate that MAS has taken on board some of AWS' key feedback from earlier consultations, such as introducing materiality as a condition for different requirements, and allowing the use of external auditors to obtain assurance on a service provider's security and control environment.

To further improve this proposed Notice, we would like to offer some comments on the (1) Consultation Paper, and the (2) Proposed Notice to Banks on Management of Outsourced Relevant Services ("Notice"). We apologize that our responses do not follow the prescribed submission format. While we have appended our detailed comments to this letter, we would like to highlight some key recommendations for your consideration:

- **Clarify the basis for inclusion or exclusion under the definition of "outsourced relevant service".** It is currently unclear what the rationale for including or excluding relevant services from Annexes B and C is (i.e. how "relevant services" would constitute an "outsourced relevant service" or an "exempted outsourced relevant service"). Specifically, we seek clarification on how "the characteristics of the service" for relevant services, such as payment card network infrastructure, would constitute their exclusion from the definition of an "outsourced relevant service". Conversely, we seek clarity on why cloud services are explicitly included as an "outsourced relevant service".
- **Avoid overly prescriptive legally binding requirements.** The mandatory requirements in this Notice are overly rigid and impose a 'one-size-fits-all' approach to all types of outsourcing without recognizing its commercial, technological and operational implications. There are several areas in the Notice where the legally binding obligations on banks would be impractical or commercially infeasible to implement for cloud outsourcing (elaborated in our detailed comments). The Notice should instead provide a risk assessment framework with high-level requirements around assessing and mitigating risk, while giving banks the discretion to address identified risks based on the nature of their business and the services they are acquiring.
- **Define the term "disclose" in Notice, as the term is not defined in the Notice or in the Banking Act.** The obligations in Section 5.1(c), 6.1 and 6.2(b) of the Notice raise the concept of disclosing customer



information to a service provider, without defining what MAS means by “disclosure”. While cloud service providers may store or process information, such information is not “disclosed” in the ordinary meaning of the term (i.e. AWS does not have visibility into our customers’ content). As such, we recommend properly defining the term to exclude the passive role of cloud service providers, as the related obligations would be impractical and overly burdensome for both banks, their customers and the service provider.

- **Avoid overly prescriptive and impractical subcontracting restrictions.** Sections 6.1, 6.2, and 7.1(h) of the Notice prescribe requirements for commercial agreements between banks and their service providers and dictate down-stream contractual agreements with third parties that are impractical to implement for cloud services. Cloud services are often homogenized and provided on a one-to-many basis; it is impractical (if not impossible) to tailor service offerings for any individual customer, and therefore infeasible for the service provider to implement different subcontractor management processes or contracts with subcontractors based on the risk assessment of each individual bank. We recommend that MAS retains the flexibility provided to banks under Section 47A(4) and (5) of the Banking Act, and the MAS Guidelines on Outsourcing.
- **Contractual rights should account for different outsourcing circumstances.** The Notice requires banks to include mandatory and broad termination rights in their outsourcing agreement, which go beyond material breach of the agreement or a regulator instruction from MAS to terminate the agreement. The terms that must be specifically stated in an agreement are ‘one-size-fits-all’ and do not account for different outsourcing circumstances. Given that non-compliance with the Notice can lead to criminal sanctions, we recommend affording banks greater flexibility in implementing appropriate and commercially viable contractual terms.
- **Review MAS audit requirements of service providers and subcontractors.** Section 7.1(d) of the Notice turns the permissive Section 47A (5)(c) and Section 47A (10) of the Banking Act into a mandatory and rigid set of contractual terms, significantly expanding the scope of MAS’s audit without affording practical protections to service providers, or their subcontractors. Instead, we recommend that MAS references the scope of audit in the MAS Guidelines on Outsourcing as a benchmark for this Notice.

We would like to clarify that our comments herein are non-exhaustive, and we would very much welcome a meeting with MAS to discuss our feedback in greater detail. Once again, we thank MAS for the opportunity to comment and stand ready to further discuss these points with MAS at your convenience.

Sincerely,

A handwritten signature in black ink, appearing to be "Genevieve Ding", written in a cursive style.

Genevieve Ding
Head of Public Policy, Singapore & Asean Strategic Projects
Amazon Web Services




Consultation Paper on Outsourcing by Banks and Merchant Banks		
Section	Issue	AWS Comments
N/A	Overly prescriptive requirements in the Notice	In contrast to other jurisdictions with respect to legally binding regulations, the proposed Notice is extremely rigid and prescriptive about contractual terms. While the recent amendments to the Banking Act grant MAS the power to impose additional steps and requirements before banks undertake outsourcing, these mandatory requirements should not be overly rigid so as to impose a ‘one-size-fits-all’ approach to all types of outsourcing without recognizing commercial, technological and operational implications. We elaborate, below, several areas where the legally binding obligations on banks in the Notice are likely to be impractical or commercially infeasible to implement for cloud outsourcing, such that banks’ full access to these services could be curtailed. A principles based approach by contrast, as adopted in the existing MAS Guidelines on Outsourcing, is an outcome-focused regulatory framework, which recognizes that an overly prescriptive approach to regulation (1) unnecessarily increases compliance costs; (2) increases the burden on regulators to constantly review and implement best practices (otherwise, risks outdated controls); and (3) encourages a “check the box” approach to measuring success. On the other hand, a prescriptive approach, which includes detailed and highly complex rules, can divert attention away from the purpose of the regulatory framework by requiring Financial Services Institutions (FSIs) to focus on adhering to the letter of the law, rather than on its intended outcome. Typically, other regulated entities provide high-level requirements while allowing their regulated entities discretion to contractually draft or implement the requirements as appropriate to the complexities of their business or the services they are acquiring.
		AWS Recommendation MAS should consider providing banks with a risk-based framework that includes suggestions on how to mitigate these risks, while ultimately allowing them the discretion to implement measures based on the nature and complexity of their business, and the services they are acquiring. In the Notice, MAS should also clearly state that risks relating to contractual terms should be addressed in substance rather than through including <i>verbatim</i> language that is lifted wholesale from this Notice.
Annex B: Proposed Notice to Banks on the Management of Outsourced Relevant Services		



Annexes B and C	Basis of inclusion under the definition of “outsourced relevant service” unclear	Annex B lists the relevant services that are excluded from the definition of “outsourced relevant service” while Annex C lists the relevant services considered as “outsourced relevant services”. Most of the services listed in Annex C are information technology related, even though the Notice is not tailored and, in some cases, is inconsistent with the way in which these services are provided to banks. It is unclear what the basis or rationale is for including or excluding relevant services from Annex B and C. For example, services such as telecommunication services, payment card network infrastructure, bill payment services, or scheduled maintenance of equipment supporting business continuity and IT disaster recovery, are excluded as “outsourced relevant services”, but there is no basis for why or how the “characteristics” of the services constitute their exclusion.	State clearly the rationale for inclusion and exclusion of services under the definition of “outsourced relevant services”.
Section 5.1(c), 6.1 and 6.2(b)	Definition of “disclosure”	The obligations in Section 5.1(c), 6.1 and 6.2(b) raise the concept of disclosing customer information to a service provider. However, the term “disclose” is neither defined in the Banking Act nor the Notice. In many cloud services contracts, information may be processed or stored by the service provider but it is not “disclosed” in the ordinary meaning of the term (i.e. there is no systemic human readable access granted to the service provider as a necessary component of providing the service, and the cloud service provider does not have visibility into its customers’ data). The obligations in Section 5.1(c), 6.1 and 6.2(b) are impractical and overly burdensome for banks, their customers and the service provider, if the term “disclosure” is interpreted broadly to cover this passive role. For example, under Section 6.1, banks will be required to seek individual written consents from their customers to use the services of cloud service providers who may use subcontractors in their service delivery from time to time. As written in the Notice, if a single customer does not consent, then the bank would not be able to use the cloud service provider’s services for that customer, even if the bank’s	We recommend clarifying the term “disclosure” so that it does not apply to such circumstances. In provisions dealing with the “disclosure” of customer information, MAS should carve out an exemption for the provision of services where there is no programmatic access to human readable data granted to the service provider, as a necessary and inalienable part of the service delivery.



		applications are reliant on the cloud service provider to function and there would be no feasible alternative to provide services to the individual.	
6.1, 6.2, 7.1(h)	Subcontracting restrictions are overly prescriptive	In addition to the obligations highlighted above with respect to “disclosure” of customer information, Section 6.2 prescribes requirements for commercial agreements between banks and their service providers that are impractical for cloud services. Cloud services are often homogenized and provided on a one-to-many basis; it is impractical (if not impossible) to tailor service offerings for any individual customer, and therefore infeasible for the service provider to implement different subcontractor management processes or contracts with subcontractors based on the risk assessment of each individual bank. As we will highlight in 7.1(d) below, we recommend that MAS retains the flexibility provided to banks under Section 47A(4) and (5) of the Banking Act and the MAS Guidelines on Outsourcing. For example, Section 6.2(b)(i) of the Notice requires cloud service providers to give individual notices to their subcontractors for each individual Singapore customer that uses their service. However, hyperscale cloud service providers typically engage subcontractors to provide services across their entire customer base, and not for individual customers. Therefore, these types of notices would not only be administratively burdensome, but they are also unlikely to achieve their intended purpose, as the subcontractor would not typically be able to distinguish the services they provide on an individual bank basis. In addition, Sections 6.2(d) and 7.1(h) of the Notice require cloud service providers to include at least one of the contractual terms listed in that section in their agreement with subcontractors, based on an individual bank’s determined preference. This provision is overly prescriptive for commercial agreements as it dictates down-stream	We recommend that, for cloud service providers, MAS removes Sections 6(d)(i) to (vi) and 7.1(h) and replaces them with an obligation to ensure that the subcontractor will keep the bank’s information confidential, and that the service provider will be responsible to the bank if the subcontractor fails to do this.

		contractual agreements with third parties. This would be impractical to implement. To address subcontracting risk, other regulators, such as the Australian Prudential Regulation Authority (APRA), require banks to conduct due diligence into their service providers' subcontracting practices, conduct ongoing monitoring, and ensure that the service provider remains contractually liable for the subcontractors' breach. MAS should consider adopting a similar framework, which will allow banks to implement measures that are appropriate to the circumstances and nature of the service(s) they are acquiring.	
7.1(g)	Rigid contractual termination rights	Section 7.1(g) of the notice removes banks' flexibility to determine the appropriate commercial terms for their outsourcing agreements. It requires banks to include mandatory and broad termination rights in their outsourcing agreement, which go beyond material breach of the agreement or a regulator instruction from MAS to terminate the agreement. The broad bases for termination also expand on those set out in the MAS Guidelines on Outsourcing, and present a rigid set of terms that must be specifically stated in an agreement. These terms are a one-size-fits-all and do account for different circumstances of outsourcing. This is different to APRA CPS 231 or the European Banking Authority (EBA)'s Outsourcing Guidelines, wherein both require outsourcing agreements to cover bank's termination rights but do not mandate the specific way the right needs to be written in contracts. The bases for termination under EBA and APRA are also narrower than those prescribed in the Notice. Given that non-compliance with the Notice can lead to criminal sanctions, we recommend affording banks greater flexibility in implementing appropriate commercially viable contractual terms.	We propose amending Section 7.1(g) to draw on the existing MAS Guidelines on Outsourcing: <i>"(g) a requirement that the bank may terminate the contract or stop obtaining or receiving the material ongoing outsourced relevant service from the service provider if instructed by the Authority, or in accordance with applicable law, which may include the following circumstances:</i> (i) <i>the service provider has materially breached its obligations of confidentiality or security in relation to the provision of</i>

			<i>the material ongoing outsourced relevant service;</i> (ii) <i>the service provider becomes insolvent or goes into liquidation;</i> (iii) <i>the service provider goes into receivership or judicial management whether in Singapore or elsewhere;</i> (iv) <i>there is a demonstrable deterioration in the ability of the service provider to perform the contracted service; and</i> (v) <i>the service provider undergoes a change in its ultimate beneficial ownership.”</i>
7.1(d)	MAS audit of service providers and subcontractors	Section 7.1(d) turns the permissive language in Section 47A (5)(c) and Section 47A (10) of the Banking Act into a mandatory and rigid set of contractual terms, significantly expanding the scope of MAS’s audit without affording practical protections to service providers, or their subcontractors. We recommend that MAS references the scope of	We recommend introducing a section stating clearly that in the first instance, MAS will work with banks to get the information necessary for its



	audit in the MAS Guidelines on Outsourcing as a benchmark for this Notice. While Section 47A(7)(c) of the Banking Act has a suggested audit scope that banks <i>may</i> include in their outsourcing agreement, the Notice makes it mandatory for all agreements to include these regulatory audit rights seemingly <i>verbatim</i>, regardless of the nature of the service. This is impractical. Moreover, the scope of Section 47A(7)(c) of the Banking Act refers only to “record, document, information or report relating to the provision of the relevant service from the person,” but the Notice has been expanded to include “systems and premises,” which seems inconsistent with the legislative intent of the audit scope when read together with Sections 47A(5)(c) and 47A(10). While we recognize that the text in this section broadly comes from the Banking Act, the audit scope requirements set out in Section 7.1(d)(i)(C) and 7.1(d)(ii) of the Notice are unusual in the context of cloud services. In the context of subcontracted cloud services, the banks have clearest visibility of how their customer information is processed and secured (please refer to AWS’ shared responsibility model at Annex, which provides an overview of the customers’ (banks’) responsibility and ability to control “security in the cloud”, including the determination of security configurations). It is not apparent how MAS would assess a service provider’s ability to manage “legal [and] reputational risk” where the service provider is providing a relatively homogenized set of services across its customer base on a global scale. Likewise, it is not apparent why MAS should have the ability to conduct audits on the “system and premises” of service providers to assess the “level of compliance of the service provider with written laws,” or have the necessary expertise to assess this, unless those laws are administered by MAS. Furthermore, audits to system and premises may disrupt the provision, availability, confidentiality and	supervisory duties. MAS will only ask for the service provider’s cooperation to provide information necessary for MAS to carry out its supervisory duties, if the banks are unable to provide the necessary information. In reaching out to service providers for more information, we further recommend deleting Section 7.1(d) and replacing it with the following, which draw on the existing MAS Guidelines on Outsourcing: <i>“(d) A requirement that the Authority, or an auditor appointed by the Authority, is able to: (i) access and inspect the service provider, and obtain records, documents, information or reports relating to the provision of the relevant service given to, stored at or processed by the service provider; and (ii) access any report and finding made on the service provider whether produced by the service provider’s internal or external auditors, or by agents appointed by the service provider in relation to the</i>
--	--	---



		security of the services provided. This may also impact other customers and have ramifications on business. Additionally, the Section 47A5(c) of the Banking Act suggests that the Notice should specify the times at which any MAS audit will be conducted, which has not been stipulated. Given that security is the highest priority for cloud service providers, we recommend in addition to the above, that the Notice specify that any audit will be carried out with reasonable notice to the service provider.	<i>material ongoing outsourced relevant service, to assess the service provider's ability to provide the material ongoing outsourced relevant service and its compliance with applicable laws administered by the Authority.</i> <i>The Authority will provide the bank reasonable notice of its intent to exercise its inspection rights and share its findings with the institution where appropriate."</i>
--	--	--	---



Annex:

AWS Shared Responsibility Model. AWS is responsible for “Security of the Cloud: and _responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. The customer is responsible for “Security in the Cloud” .Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities

