

Banking Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Fax: (65) 62203973
Email: outsourcing@mas.gov.sg

5 Feb 2021

Dear sir/madam,

Re: ACCA comments to the Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services

The Asia Cloud Computing Association (ACCA) thanks the Monetary Authority of Singapore for the opportunity to comment on the abovementioned Notice.

As the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem, we represent a vendor-neutral voice of the private sector to government and other stakeholders. Our mission is to accelerate the adoption of Cloud computing through Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for Cloud computing products and services. We are committed to strengthening the cybersecurity resilience and developing a robust technology ecosystem which supports a vibrant digital economy.

In consultations with our members, we are submitting comments on the **Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services**.

As some of the feedback provided goes into some detail, we would like to request for a meeting with the MAS to explain our submission. Please let us know if you are available for this meeting (by videoconference) on **24 Feb 2021, Wednesday, 10am**, or if an alternative date/time would be more suitable.

Thank you again for the opportunity to respond to this Notice, and I look forward to hearing from you on our meeting request.

Yours sincerely,
Lim May-Ann
Executive Director
Asia Cloud Computing Association


Table of Contents

General Comments	4
Question 1 MAS seeks comments on the proposed annexes of the proposed Notices	5
Location(s): Appendix B, Annex A, 1.(xiv)	5
Observation(s)	5
Recommendation(s)	5
Location(s): Appendix B: Annexes B and C	6
ACCA observation(s)	6
Recommendation(s)	6
Location: Appendix B: Section 5.1(c), 6.1 and 6.2(b)	6
Observation(s): 5.1(c), 6.1, 6.2(b)	6
Recommendation(s)	6
Observation(s): 6.1(b)	7
Recommendation(s)	7
Location(s): Appendix B: 6.1, 6.2, 7.1(d), 7.1(h)	8
Observation(s): 6.1, 6.2, 7.1(d)	8
Recommendation(s)	8
Observation(s): 6.2(d), 7.1(d)	9
Recommendation(s)	9
Observation: 6.2(d)(iv)	10
Recommendation:	11
Location(s): Appendix B: 6.3(a)	11
Observation(s)	11
Recommendation(s)	11
Location(s) Appendix B: 7.1(g)	11
Observation(s)	11
Recommendation(s)	12
Location(s): Appendix B: 7.1(d)	12
Observation(s)	12
Recommendation(s)	12
Observation(s)	12
Recommendation(s)	13
Locatio(s): 7.1 (g)(iii) and (iv)	13
Observation(s)	14
Recommendation(s)	14
We suggest paragraph 7.1(g)(iii) and (iv) be amended as follows:	14
Location: Appendix B: 9.1	14
Observation(s)	14
Recommendation(s)	14

Location: Annex C, 1.....	15
Observation(s).....	15
Recommendation(s)	15
Question 5 MAS seeks comments on the terms required to be included in the outsourcing agreements.....	15
Outsourcing Agreement Terms	15
Observation(s) and Recommendation(s)	15
Question 6 MAS seeks comments on the requirements pertaining to the protection of customer information.....	16
Observation(s).....	16
Question 7 MAS seeks comments on the requirements pertaining to the use of subcontractors for material ongoing outsourced relevant services	16
Observation(s).....	16
Recommendation(s)	16
Question 8 MAS seeks comments on the requirements pertaining to the audit requirements for material ongoing outsourced relevant services	17
Observation(s).....	17
Recommendation(s)	17

ACCA comments to the Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services

General Comments

The ACCA notes that in contrast to other jurisdictions with respect to legally binding regulations, the obligations on banks in the proposed Notice is extremely rigid and prescriptive.

While the recent amendments to the Banking Act grant the 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 in our submission below, several areas where the legally binding obligations on banks in the Notice are likely to be impractical to implement for cloud outsourcing, or will be commercially infeasible to implement, such that banks' full access to these services could be curtailed.

A principles-based approach by contrast, as adopted in the existing MAS Outsourcing Guidelines, is an outcome focused regulatory framework and recognizes that 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 (or else risk outdated controls), and (3) encourage a "check the box" focus, rather than a focus on implementing the best possible outcome.

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 FSIs to focus on adhering to the letter of the law.

Other regulators therefore typically provide high-level requirements while allowing their regulated entities discretion to contractually draft or implement the requirements.

MAS should consider providing Banks with a risk framework and 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.

MAS should also state clearly in the Notice that requirement relating to contractual terms should be addressed in substance and in principle rather than requiring inclusion of verbatim language that is lifted wholesale from this Notice.

Question 1 MAS seeks comments on the proposed annexes of the proposed Notices

Location(s): Appendix B, Annex A, 1.(xiv)

“marketing or research conducted in the name of the bank or cobranded with the name of the bank, or where such marketing or research involves the bank’s confidential information or customers’ information,”

Observation(s)

The ACCA notes that the current wording of the activity is broad and may be taken to include not just marketing activities directly undertaken on behalf of the bank by intermediaries, but also more general activities such as:

- purchasing online digital marketing advertising space and related analytics services, which are not typically performed by banks; and
- co-marketing activities undertaken with partners which do not consider themselves as providing an outsourced service to the bank or in a typical principle/service provider relationship.

We do not believe it is MAS’ intent - nor is it accurate - to indicate that such purchase of online digital advertising space and related marketing analytics activities are typically performed by banks and therefore in scope of the definition of Outsourced Relevant Services.

We similarly do not believe it is MAS’s intent to indicate that co-marketing activities with partners should be considered Outsourced Relevant Services since by definition these are not activities the bank could conduct on their own absent such partner.

These services are conducted by third party providers or partners and would not be undertaken by banks. It would therefore be useful to both parties to set out this clarification in Annex A (list of relevant services commonly performed by banks or MBs in Singapore).

Recommendation(s)

We suggest Annex A, 1. (xiv) be amended as follows: “marketing or research conducted in the name of the bank or cobranded with the name of the bank, or where such marketing or research involves the bank’s confidential information or customers’ information, excluding general digital advertising and marketing analytics services purchased by the bank; and co-marketing activities (i.e. activities wholly or partly intended to promote a partner’s own products or services) undertaken with a partner;”

Alternatively, and preferably, we suggest the exclusion indicated in the blue text above be included as an insertion in Annex B paragraph 1, in light of the fact that Annex A is a non-exhaustive list of what are outsourced relevant services. Strictly speaking, excluding digital ad services etc from Annex A would not necessarily mean they are not outsourced relevant services, while Annex B provides for clear, express exclusions.

Location(s): Appendix B: Annexes B and C

ACCA observation(s)

The ACCA notes that the basis of inclusion under the definition of “outsourced relevant service” is 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 the basis for these services being excluded due to “the characteristics of the service” is unclear.

Recommendation(s)

The ACCA recommends that MAS state clearly the rationale for inclusion and exclusion of services under the definition of “outsourced relevant services”.

Location: Appendix B: Section 5.1(c), 6.1 and 6.2(b)

Observation(s): 5.1(c), 6.1, 6.2(b)

We note that in the definition of “disclosure”, the obligations in Section 5.1(c), 6.1 and 6.2(b) turn on the concept of “disclosing” bank customers’ information to a service provider/subcontractor. However, the term “disclose” is not defined in the Banking Act or the Notice. In many cloud services contracts, while information may be processed or stored by the service provider it is not “disclosed” in the ordinary meaning of the term, i.e. is the service provider/subcontractor does not have programmatic access to human readable customer information as a necessary part of providing the service.

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 the provision of data to a CSP/subcontractor for processing. 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 the delivery of the service from time to time. As drafted, if a single customer of a single bank does not consent, then the bank would not be able to use the cloud service provider’s services for that customer (which de facto may mean not being able to use the service at all for any customers).

Recommendation(s)

We make two recommendations:

1. Clarifying the term “disclosure” so that it does not apply to such circumstances: in the provisions dealing with “disclosure” of customer information, exclude the provision of data where the service provider/subcontractor does not have programmatic access to human readable customer information as a necessary part of performing the service. The MAS could also consider defining the term “disclosure.”
2. Not requiring written consent of customers where a sub-contracting arrangement may involve disclosure of customer information, i.e. amend 6.1(b) to read “where the sub-contracting arrangement requires the disclosure of customer information, the service provider is legally responsible for the sub-contractor’s compliance with the terms in [6.2(b)].”

Observation(s): 6.1(b)

Related, we recognize that sub-contracting arrangements that require the disclosure of customer information are more sensitive and should be given closer consideration by banks. However, we believe this is achieved by the risk management requirements in Section 6.2, which include specific requirements for sub-contracting arrangements that involve the disclosure of customer information to a sub-contractor.

An additional customer consent requirement for sub-contractors would be onerous for banks and could be potentially detrimental to its customers. For example: given that many banks and service providers operate a one-to-many service model, if a handful of customers do not provide consent, a bank could potentially be blocked from implementing a sub-contracting arrangement that would ultimately provide benefits to all its customers (e.g. 24/7 customer support).

At the same time, an additional customer consent requirement for sub-contractors is arguably inconsistent given that banks are not required in the Notice to obtain customer consent to use the primary service provider. It would also go beyond sub-contracting requirements in the equivalent frameworks in the EU and the US and could place Singaporean banks at a competitive disadvantage (see [EBA Outsourcing Guideline - Sub-outsourcing of critical or important functions](#) and [FFIEC Outsourcing Technology Service - Contract Issues](#)).

If the Notice continues to require customer consent, we suggest that it should clarify that this consent can be general (i.e. for subcontractors generally as opposed to specific, named subcontractors). We believe this is MAS’ intent as this would provide the bank’s customers with visibility and protection without also creating an onerous and impractical requirement for the bank to obtain customer consent for each individual subcontractor, which could be confusing for the bank’s customers.

Recommendation(s)

We suggest paragraph 6 be amended as follows:

~~6.1 A bank in Singapore must not allow a material ongoing outsourced relevant service to be sub-contracted unless—
(a) the sub-contracting arrangement does not involve any disclosure of customer information; or~~

~~(b) where the sub-contracting arrangement requires the disclosure of customer information, the bank has obtained the consent in writing of the customer or, if he is deceased, his appointed personal representative, for it to disclose the customer information to the service provider or the sub-contractor, as the case may be.~~

~~6.2 Before obtaining or receiving any material ongoing outsourced relevant service where sub-contracting arrangements are not prohibited under paragraph 6.1 or by the outsourcing agreement, the bank must –~~

Location(s): Appendix B: 6.1, 6.2, 7.1(d), 7.1(h)

Observation(s): 6.1, 6.2, 7.1(d)

As mentioned above, the ACCA notes that the 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, and in the case of hyperscale cloud services it is generally impossible to tailor service offerings for any individual customer. Therefore it is not feasible for the service provider to implement different subcontractor management processes or contracts with those subcontractors based on the risk assessment of each individual bank. As highlighted in 7.1(d) below, we recommend that MAS retains the flexibility provided to Banks under Section 47A(4) and (5) and the MAS Outsourcing Guidelines in managing subcontracting risk.

For example, 6.2(b)(i) of the Notice requires cloud service providers to give notice to each of their subcontractors when a customer that is a licensed bank or MB uses their services to process data. However, hyperscale cloud service providers typically engage subcontractors to provide services across their entire customer base in different sectors and geographies. The content and nature of data processed by CSPs (and their subcontractors) for financial institutions and other customers is not visible to CSPs, and therefore all of the data is handled in accordance with the same standards, policies, and processes. Therefore these types of notices would not only be administratively burdensome, but they are also unlikely to achieve their intended purpose.

In addition, 6.2(d) and 7.1(h) of the Notice requires 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 and because it aims to dictate down-stream contractual agreements with third parties, it is impractical to implement.

To address subcontracting risk, other regulators such as the Australian Prudential Regulation Authority 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 because it will allow banks to implement measures that are appropriate to the circumstances and nature of the service they are acquiring.

Recommendation(s)

We recommend that for cloud service providers MAS removes paragraphs 6.2 (b) - (d) and 7.1(h) and replaces them with an obligation for the service provider to contractually commit to be responsible to the bank for subcontractors' compliance with the relevant outsourcing agreement terms relating to confidentiality, privacy, and data protection, including all relevant requirements specified in the Notice.

Observation(s): 6.2(d), 7.1(d)

6.2(d) and 7.1(d) duplicates Section 7.1 for the outsourcing agreement and may lead to the same duplication in outsourcing contracts as banks feel they need to address both the requirements for the primary service provider and the sub-contractor separately. This will further extend the contract negotiation process without providing additional safeguards in practice.

The approach in other outsourcing frameworks (including in the EU and the United States) is to address sub-contractor agreements by requiring providers to ensure that their sub-contractors comply with the relevant and applicable provisions in the outsourcing agreement (see [EBA Outsourcing Guideline - Sub-outsourcing of critical or important functions](#) and [FFIEC Outsourcing Technology Service - Contract Issues](#)). This provides the necessary protection whilst also allowing providers a degree of flexibility to ensure that the requirements are addressed in their sub-contractor agreements without the primary outsourcing agreement dictating the precise contract language that must be used between the service provider and the sub-contractor. This is important given that in many contexts - including in the context of public cloud services - sub-contracting arrangements are often in place before the outsourcing agreement is signed.

Recommendation(s)

We suggest paragraph 6.2(d) be amended as follows:

6.2 Before obtaining or receiving any material ongoing outsourced relevant service where sub-contracting arrangements are not prohibited under paragraph 6.1 or by the outsourcing agreement, the bank must – ...

(d) if the bank determines that a sub-contracting agreement is required under paragraph (c), ~~determine whether it is necessary for the bank to~~ include in its outsourcing agreement, a requirement that the service provider ensures that its sub-contractors comply with all relevant contractual obligations in the outsourcing agreement. ~~ensures that a sub-contracting agreement includes, any one or more of the following:~~

- ~~(i) a requirement that the sub-contractor protects the confidentiality and integrity of all information of the bank in its custody, in relation to the provision of the relevant service under the sub-contracting arrangement;~~*
- ~~(ii) a requirement that the sub-contractor ensures that it and its employees only access, collect, copy, modify, use, store, or process any customer information of the bank to the extent that is necessary for it and its employees to provide the relevant service under the subcontracting arrangement;~~*
- ~~(iii) a requirement that the sub-contractor ensures that it and its employees do not disclose any customer information of the bank to any third party unless compelled by~~*

~~law, in which case the subcontractor must notify the bank directly or through the service provider as soon as practicable to the extent permitted by law;~~
~~(iv) a requirement that the Authority, or an auditor appointed by the Authority, be allowed to audit the books, systems and premises of the sub-contractor for the purposes of determining whether the sub-contractor is properly providing the relevant service, properly providing the relevant service under the subcontracting arrangement and assessing—~~
~~(A) the ability of the sub-contractor to—~~
~~(I) ensure continuity of the relevant service under the subcontracting arrangement;~~
~~(II) safeguard the confidentiality and integrity of all information in its custody, in relation to the provision of the relevant service under the sub-contracting arrangement; and~~
~~(III) manage its legal, reputational, technological and operational risks arising from the provision of the relevant service under the sub-contracting arrangement; and~~
~~(B) the level of compliance of the sub-contractor with written laws related to the provision of the relevant service under the subcontracting arrangement;~~

We suggest paragraph 7.1(d) be amended as follows:

For the purposes of section 47A(2)(b) and 47A(4)(b) of the Act, before obtaining or receiving a material ongoing outsourced relevant service, a bank in Singapore must enter into an outsourcing agreement, which must include all of the following:

- (d) a requirement that the Authority, or an auditor appointed by the Authority, be allowed to audit the relevant information ~~books~~, systems and premises of the service provider used to provide the ongoing outsourced relevant service for the purposes of determining whether the service provider is ~~properly providing~~ complying with the ~~material ongoing outsourced relevant service~~ outsourcing agreement and assessing
- (i) the ability of the service provider to –
- (A) ensure continuity of the material ongoing outsourced relevant service;
- (B) safeguard the confidentiality and integrity of all information in its custody, in relation to the provision of the material ongoing outsourced relevant service; and
- (C) manage its legal, reputational, technological and operational risks arising from the provision of the material ongoing outsourced relevant service; and
- (ii) the level of compliance of the service provider with written laws related to the provision of the material ongoing outsourced relevant service;

Observation: 6.2(d)(iv)

As currently drafted, this paragraph does not expressly limit the access and audit right to the books, systems and premises actually used by the sub-contractor to provide the outsourced services to the bank. In addition, the references to “books” and “properly providing the relevant service” are unclear in an IT context.

Not all the provider’s information, systems and premises will necessarily be relevant to the outsourced services provided to the bank, and so relevant to any assessment by or on behalf of the outsourcing bank. Any right to access or audit should be expressly limited to the information, systems and premises which are actually used to provide the service to the outsourcing bank.

In addition, we suggest the reference to “books” is replaced with a reference to “information” and the reference to “properly providing the relevant service” be replaced with a reference to compliance with the outsourcing agreement, as the agreement describes the service provider’s obligations vis-a-vis the bank.

Recommendation:

We suggest the following amendment to 6.2(d)(iv) –

a requirement that the Authority, or an auditor appointed by the Authority, be allowed to audit the relevant information ~~books~~, systems and premises of the sub-contractor used to provide the ongoing outsourced relevant service for the purposes of determining whether the sub-contractor is ~~properly providing~~ complying with the relevant service all relevant contractual obligations. ~~properly providing the relevant service under the subcontracting arrangement and assessing—~~

Location(s): Appendix B: 6.3(a)

Observation(s)

We note that the Notice has an overly prescriptive timeframe to notify of subcontractor engagement. The requirement to notify Singapore banks within 30 days of the engagement of a sub-contractor (typically on a global basis) is arbitrary and unnecessarily prescriptive. For various reasons it may not always be possible for a CSP to notify a bank of engagement of a subcontractor precisely within a 30-day timeframe of the engagement.

Recommendation(s)

Presumably the purpose is to provide time for the bank to determine whether any assessment or other measures are necessary once the subcontractor is identified. We recommend amending the language to reflect this principle” to replace the 30-day notification requirement with the following: “(a) the bank is notified of the engagement of a subcontractor within a reasonable amount of time in advance of advance of the subcontractor’s authorization to perform services that may involve access to customer information.”

Location(s) Appendix B: 7.1(g)

Observation(s)

We note that the Rigid Contractual Termination Rights in 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 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 Outsourcing Guidelines, 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 not take into account different circumstances of outsourcing. This is different from APRA CPS 231 or the EBA's Outsourcing Guidelines - both require outsourcing agreements to cover bank's termination rights but do not mandate the specific provisions that must be included. 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.

Recommendation(s)

We recommend the following changes to 7.1(g), which draw on the existing MAS Outsourcing Guidelines:

(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:

the service provider has materially breached its obligations of confidentiality or security in relation to the provision of the material ongoing outsourced relevant service;

- i. the service provider becomes insolvent or goes into liquidation;*
- ii. the service provider goes into receivership or judicial management whether in Singapore or elsewhere;*
- iii. there is a material and demonstrable deterioration in the ability of the service provider to perform the contracted service; and*
- iv. the service provider undergoes a change in its ultimate beneficial ownership.*

Location(s): Appendix B: 7.1(d)

Observation(s)

In the MAS Audit of service providers and subcontractors, the ACCA notes that 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 and significantly expands the scope of MAS's audit without affording practical protections to service providers, or their subcontractors.

Recommendation(s)

We recommend that MAS takes into account the scope of audit contained in the MAS Outsourcing Guidelines as a benchmark for this Notice.

Observation(s)

While the Banking Act section 47A(7)(c) has a suggested audit scope that banks *may* include in their outsourcing agreement, the Notice makes it mandatory for all agreements to include these regulatory audit rights seemingly *verbatim*, 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 does not seem consistent 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) 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. It is not apparent how MAS would assess a service provider’s ability to manage “legal [and] reputational risk” to its regulated entities where the service provider is providing a relatively homogenized set of services across its customer base on a global scale across sectors. 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.

Recommendation(s)

Additionally, the Banking Act section 47A(5)(c) 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 specifies that any audit is carried out with reasonable notice to the service provider.

We recommend introducing a section stating clearly that in the first instance, MAS will work with banks to get the information necessary for its 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 Outsourcing Guidelines:

(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 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.

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.

Locatio(s): 7.1 (g)(iii) and (iv)

Observation(s)

It is unclear why there should be an explicit termination right (and notification obligation) just because a sub-contractor has undergone or is undergoing a change of control or is insolvent etc.

The primary service provider has the direct relationship with the bank and responsibility for the service. A change to the primary provider's ownership or financial viability could realistically be assumed to impact service delivery and / or risk such that a termination / notification requirement is justifiable.

However the same is not true of sub-contractors - especially given how widely that term is defined in the Notice ("any part of the relevant service"). A change of ownership or financial status of a sub-contractor should not give rise to a termination right where there is not also a deterioration in the service - and the latter point is already addressed in sub-section (iv). Banks should not be expected to monitor the status of sub-contractors unless there is an identifiable impact on the relevant service.

Recommendation(s)

We suggest paragraph 7.1(g)(iii) and (iv) be amended as follows:

For the purposes of section 47A(2)(b) and 47A(4)(b) of the Act, before obtaining or receiving a material ongoing outsourced relevant service, a bank in Singapore must enter into an outsourcing agreement, which must include all of the following:

(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 under any of the following circumstances:

(iii) the service provider ~~or a sub-contractor, as the case may be~~, has undergone or is undergoing a change in ownership, is insolvent, has gone or is going into liquidation or receivership;

(iv) there has been a deterioration in the ability of the service provider or a sub-contractor, as the case may be, to provide the material ongoing outsourced relevant service in accordance with the outsourcing agreement or sub-contracting arrangement respectively;

Location: Appendix B: 9.1

Observation(s)

On independent audits, Section 9.1 requires that the bank ensure that independent audits are conducted on material ongoing outsourced relevant services at least every 3 years.

Recommendation(s)

The ACCA recommends clarifying that banks do not have to procure such audits themselves, but can rely on independent audits procured by service providers. i.e. to add a sentence at the end of 9.1 as follows: "Banks may rely on third-party independent audits procured by the service providers."

Location: Annex C, 1.

Observation(s)

On public cloud services such as software-as-a-service, platform-as-a-service, infrastructure-as-a-service, the ACCA notes that not all public cloud services should be automatically deemed as "Outsourced Relevant Services".

Public cloud services cover a broad spectrum of services. Depending on the scope or functionality of a cloud service, it may or not satisfy the definition of Outsourced Relevant Services. A service that would not be an Outsourced Relevant Service if it were performed in a non-cloud environment should not be deemed an Outsourced Relevant Service simply because it is provided using cloud technology. This would unduly expand the scope of Outsourced Relevant Services beyond the boundary of the definition in the Notice.

It would be disproportionate to deem all public cloud services as within the definition of "Outsourced Relevant Services" without consideration of the specific type of service and whether it actually satisfies the definition. It would also be inconsistent with the approach taken by other regulators notably in the EU and the United States. Doing so would unduly increase the burden on banks, supervisors and providers and could place Singaporean banks at a competitive disadvantage.

Recommendation(s)

We suggest amending Annex C, 1. as follows:

Public cloud services such as software-as-a-service, platform-as-a-service, infrastructure-as-a-service, to the extent used for a service that:
(a) is performed by a bank or was performed by a bank at any time prior to it obtaining or receiving the relevant service; or
(b) is commonly performed by banks in Singapore;

Question 5 MAS seeks comments on the terms required to be included in the outsourcing agreements

Outsourcing Agreement Terms

Observation(s) and Recommendation(s)

The ACCA agrees with the general principle of requiring certain issues to be covered in outsourcing agreements; however, we recommend that MAS avoids prescribing specific provisions to be included.

While the ACCA does not take issue with requiring service providers to enter into written agreements with their subcontractors, (i) this is a due diligence/compliance issue, which is not suited to be covered in an outsourcing agreement; and (ii) given the volume and confidentiality of such agreements to which the bank/merchant bank is not a party, it should not be required to share such agreements with the bank/merchant bank.

Further, if the service provider is willing to accept legal responsibility for its subcontractors' compliance with the outsourcing agreement terms, there is no need to prescribe any form of subcontract, or any specific terms.

Question 6 MAS seeks comments on the requirements pertaining to the protection of customer information

Observation(s)

The ACCA understands that the term “customer information” refers to customers of the banks/MBs. Hyperscale cloud service providers (CSPs) acting as data processors generally handle all of the bank’s/MB’s data to the same high standard. They do not have visibility into the content of the data and therefore do not and cannot treat certain categories of the bank’s/MB’s data differently.

Question 7 MAS seeks comments on the requirements pertaining to the use of subcontractors for material ongoing outsourced relevant services

Observation(s)

This is a key issue which will be addressed in further detail below in the context of the relevant provisions in the Notices.

Recommendation(s)

There are three sub-issues which the ACCA requests that MAS clarify:

- (1) **Disclosure:** The concept of bank secrets and related laws in many jurisdictions should be updated to reflect how data is used today. The term “disclosure” should be clearly defined within that context. If data is not readable or usable by humans, as discussed further below, then the provision of data alone (e.g. for processing) should not constitute “disclosure” considering the harm that Section 47 of the Banking Act is seeking to address.
- (2) **Subcontractors:** The ACCA understands from previous discussions with MAS that the term “subcontractors” with respect to CSPs is intended to mean companies that the CSP retains to take over performance of part or all of a cloud service. We understand it is not intended to apply to augmented/contingent staff, although such individuals may not be employees of the CSP. We recommend that the definition of subcontractors be clarified accordingly if that is indeed the intended meaning of the term with respect to CSPs.
- (3) **Need for Banks’/MBs’ customers’ consent:** The proposed notices will require written consent by all the Bank’s/MB’s customers if customer information is disclosed to any subcontractor of the CSP. Even if the definitions of “disclosure” and “subcontractors” are appropriately clarified, this is simply not a feasible option for Banks/MBs using hyperscale cloud services – nor is it necessary. For example, CSPs may subcontract support services. Depending on the definition of “disclosure” and the nature of any troubleshooting, it is possible that in certain (limited) situations customer information may be “disclosed” to such subcontractors. It is not feasible, or meaningful, to obtain

written consent in advance from all bank/MB customers for such subcontractor functions (which are not sector- or institution– specific). The ACCA recommends that instead of a written consent requirement it should be sufficient for CSPs to contractually commit to take legal responsibility for subcontractors' compliance with all requirements, including privacy, confidentiality, and data protection requirements, in the outsourcing agreement (which should meet the requirements in the Notice).

Question 8 MAS seeks comments on the requirements pertaining to the audit requirements for material ongoing outsourced relevant services

Observation(s)

Banks/MBs will be required to have independent audits conducted on all material ongoing outsourced relevant services at least every 3 years. The consultation paper clarifies that Banks/MBs may rely on “pooled audits or third-party certification performed by independent parties.”

Recommendation(s)

The ACCA recommends that MAS clarify that the latter category includes third-party audits that CSPs have conducted typically on an annual basis, e.g. SOC 2 audits.