7 October 2014

Feedback to MAS Consultation Papers on Outsourcing

Consultation Paper (P018-2014) on Notice on Outsourcing dated September 2014

Consultation Paper (P019-2014) on Guidelines on Outsourcing dated September 2014

Submitted by

ATMD Bird & Bird

SCCA Singapore Corporate Counsel Association

Bird & Bird

Feedback to the Monetary Authority of Singapore (MAS) Consultation Papers

- Consultation Paper (P018-2014) on Notice on Outsourcing dated September 2014
- Consultation Paper (P019-2014) on Guidelines on Outsourcing dated September 2014

("*Proposed Guidelines and Notice*")

TABLE OF CONTENTS

BACKGROUND

On 30 September 2014, the Singapore Corporate Counsel Association organized a dialog session for financial institutions and vendor organizations to discuss and identify common key feedback points on MAS's proposals to raise the outsourcing risk management practice standards of financial institutions.

Following the dialog session which was led by ATMD Bird & Bird, we have prepared this document to set out the feedback points which were raised and discussed at the session for MAS's informational and discussion purposes.

Although the proposed Guidelines and Notice on Outsourcing apply across all types of outsourcing and is not limited to IT outsourcing, this paper discusses MAS's proposals in the context of technology outsourcing, particularly in the context of shared services and cloud computing services, to illustrate some of the concerns of both financial institutions and their service providers.

FEEDBACK

Financial institutions (FIs) adopt shared and/or cloud services to take advantage of the cost savings, flexibility and scalability typically associated with such services, and to cater to consumer preferences which are increasingly shifting away from the traditional brick-and-mortar mode of banking in favour of the convenience of internet and mobile banking facilities.

Although the Proposed Guidelines and Notice do not prohibit FIs from engaging cloud service providers, the substance of the Proposed Guidelines and Notice would effectively rule out the adoption of cloud services by FIs.

This set of feedback has general application even though it uses cloud services to illustrate the operation of the Proposed Guidelines and Notice. It is hoped that this feedback would help achieve a proper balance between risk management and innovation.

FEEDBACK #1

"Minimum standards" should be applicable to all institutions and be measurable.

The Notice "*defines a set of minimum standards for outsourcing management*" that is legally enforceable. Thus, the Notice must specify with precision these minimum standards that are applicable to all FIs subject to MAS regulation.

A minimum standard is one which is generally applicable across the industry and is not FI specific. From an information security perspective, "standards" are distinguished from "guidelines", in that the former is more precise and tells exactly the reader what standards to adopt. The need for precision is even more pertinent when standards are legally enforceable standards.

Request: Within the Notice, we request that MAS consider removing qualitative words such as "prudently", "proper", "adequate" and words of similar effect. Further, for precision, all obligations in the Notice should be set out in a specific and measurable way.

Reference:

Proposed Notice, paragraph 3

3. Management of Material Outsourcing Arrangements

"3.1 An institution shall manage all its material outsourcing arrangements prudently. When managing such material outsourcing arrangements, the institution shall, at the minimum:

(a) establish proper policies and processes to identify all material outsourcing arrangements;

(b) put in place an adequate risk management framework, systems, policies and processes to assess, control and monitor its material outsourcing arrangements. These include establishing proper approving authorities and limits for material outsourcing arrangements;
(c) ensure that the laws, rules, regulations, notices and directives applicable to the institution continue to be complied with notwithstanding its material outsourcing arrangements; and
(d) maintain a central register of all material outsourcing arrangements.

3.2 An institution shall maintain adequate documentation of the steps taken in complying with paragraph 3.1 and furnish such documentation to MAS upon request." [Emphasis added]

Comments:

The use of words such as "prudently", "proper" and "adequate" introduce uncertainty as it is not clear what would constitute prudent, proper or adequate conduct. In the context of "minimum standards", this introduces a large degree of uncertainty for FIs as it is not clear what minimum adequate policies, processes and risk management frameworks must be adopted in order for FIs to comply.

Further, certain obligations in the Notice must be rephrased to be more specific. For example, while paragraph 3.1(c) of the proposed Notice requires FIs to simply "ensure" that FIs continue to comply with the applicable laws, the Notice does not specify how FIs are expected to do so. This requirement is too vague and not measurable.

Minimum standards must be measurable. They must be capable of being checked. Otherwise, the Notice would simply lead to an increase in regulatory risks for FIs.

Bird & Bird

FEEDBACK #2

The set of minimum standards must be capable of being complied with at all times.

The legally enforceable set of minimum standards in the proposed Notice must be capable of being complied with by the FIs at all times. Otherwise, FIs are simply set up to fail. The Notice contains several obligations which are not realistic or do not accord with industry practice. FIs would face tremendous difficulties with compliance.

Request #1: MAS should consider, upon assessment of impact to the industry:

(1) subjecting all service providers who do business with regulated FIs to MAS's purview;
(2) providing model clauses in the Guidelines for inclusion into outsourcing agreements; and
(3) relying on established IT security certifications in lieu of physical inspection or request for documents.

Reference:

Proposed Notice, paragraph 5

"An institution shall include in all its outsourcing agreements provisions that:

(a) allow the institution to conduct audits on the service provider and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to

the outsourcing arrangement and to allow such copies of any report or finding to be submitted to the Authority;

(b) allow the Authority, or any agent appointed by the Authority, where necessary or expedient, to exercise the contractual rights of the institution to access and inspect the service provider and its sub-contractors, and the institution, to obtain records and documents of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-contractors, and the right to access and obtain any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider, in relation to the outsourcing arrangement; ..."

Proposed Guidelines, paragraph 5.9.2

"An institution should include in all its outsourcing agreements clauses that:

(b) allow the institution to conduct audits on the service provider and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's or its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractor, in relation to the outsourcing arrangement;

(c) allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the institution to access and inspect the service provider and its sub-contractors, and the institution, to obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-contractors, and the right to access any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to the outsourcing arrangement; ..."

Proposed Guidelines, paragraph 5.9.3

"*<u>The outsourcing agreement should also include clauses that require the service provider to comply</u>, as soon as possible, <u>with any request from MAS or the institution</u>, to the service provider and its sub-contractors <u>to submit any reports on the security and control environment</u> of the service provider and its sub-contractors, in relation to the outsourcing arrangement*." [Emphasis added]

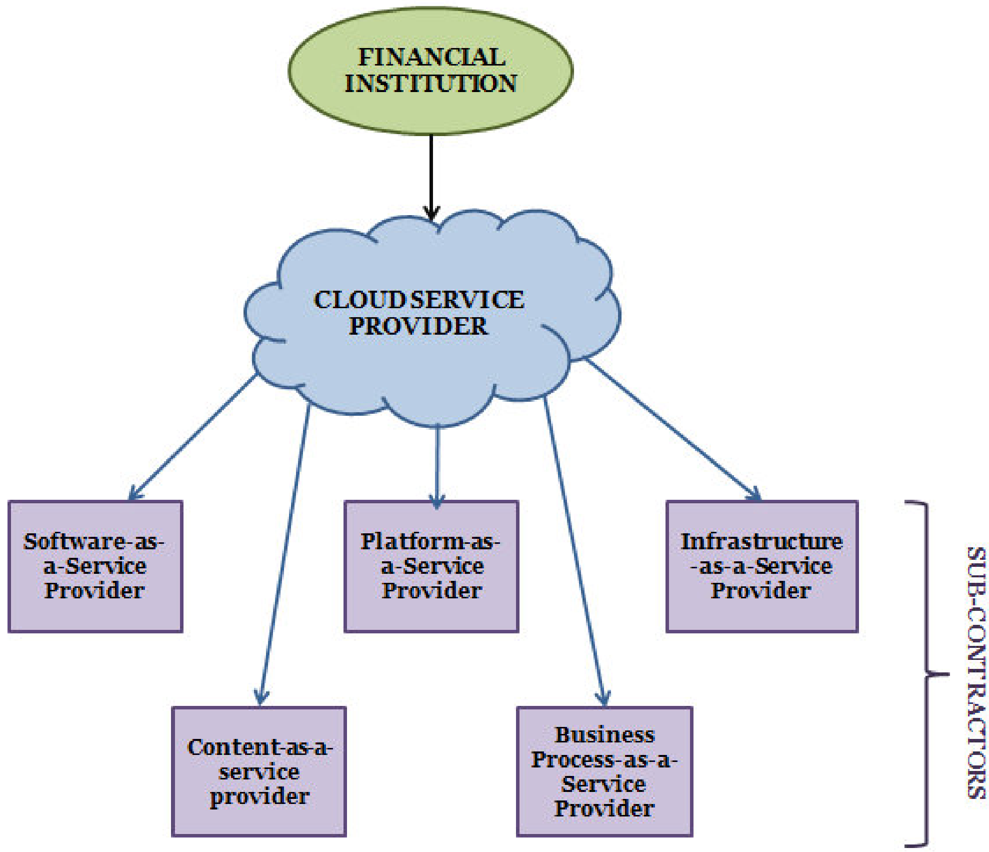
Comments:

Without a doubt, the Notice is law that is applicable to FIs. The same however cannot be said of service providers. Strictly, service providers are not subject to the Notice. Subjecting them to the Notice by way of contract erroneously assumes that FIs always have the bigger bargaining power. It also erroneously assumes that there will always be ready substitutes, or that service providers will not exit the Singapore market. The Notice inevitably sets FIs up to fail.

Even if service providers are willing to agree to subject themselves to the Notice, and agree to the inclusion of the proposed provisions without amendment, they might still for legitimate reasons, such as for confidentiality, unable to comply with the proposed provisions.

Also, the proposed provisions are onerous in that they assume the service providers always have the requisite control or power over their sub-contractors. Sub-contracting is often a complicated business and services providers may or may not have the requisite control or power over their sub-contractors. Please see for example, European Commission, 'Cloud Computing Contracts – Discussion Paper on Subcontracting' dated March 25, 2014 by Isabell Conrad, Maria-Urania Dovas, Federica Poggioli, Robert Selk, Susann Wolfgram, http://ec.europa.eu/justice/contract/files/expert_groups/ expert_group_subcontracting_discussion_paper_en.pdf

Cloud relationships can potentially be extremely complex. For example, in the context of a financial institution that engages one service provider for a variety of cloud services, the figure below illustrates some of the typical categories of sub-contractors involved in the provision of the cloud services:-



In practice, the above provisions in the proposed Guidelines and Notice would mean that the FI would have to impose contractual obligations on its cloud service provider to extract, from each and every such sub-contractor, the rights of audit and access for the FI and MAS.

This poses a challenge particularly in the context of the multi-tenancy architecture commonly adopted in the cloud, as there is typically a co-mingling of data from various customers residing in the same system, service providers and their sub-contractors are also likely to resist providing the requisite rights of audit and access as the exercise of such rights may result in issues relating to confidentiality and potential unauthorised disclosure of information of the cloud service provider's other customers.

Bird & Bird

Cloud service providers generally do not disclose the whereabouts of their data centres to customers. If MAS's objective is to protect the confidentiality of customer information, a better alternative is to rely on established IT security standards and certifications such as ISO 27001 standard on information security management, iDA's Multi-Tier Cloud Security Standard (MTCS), or even the ISO/IEC 27018 standards for cloud service providers.

Request #2: To remove paragraph 6.3 from the proposed Notice.

Reference:

Proposed Notice, paragraph 6.3

"*An institution shall engage service providers that operate in jurisdictions which generally uphold confidentiality provisions and agreements. Where customer information is to be disclosed, an institution required by any law or regulation administered by the Authority to protect or not to disclose such customer information, shall obtain appropriate legal advice in respect of the overseas jurisdiction where the outsourcing arrangement is to be performed. The legal advice shall in particular highlight the circumstances under which the customer information may be required by law to be disclosed by the service provider notwithstanding any obligation of confidentiality assumed by the service provider. An institution shall regularly update its legal advice and inform its customers of the circumstances under which customer information might be so disclosed.*" [Emphasis added]

Comments:

It is onerous to impose on FIs a duty to obtain legal advice (with regard to requirements for disclosure of customer information) in respect of all overseas jurisdictions where outsourcing is to be performed.

In the context of cloud services, a cloud service provider's operations, as well as any outsourced data centres hosting the FI's customer information, may be located in multiple jurisdictions. In practice, a cloud service provider would also typically seek to secure, as part of its business strategy, the flexibility of allocating resources from different jurisdictions from which to provide its services to customers.

However, based on the above paragraph in the proposed Notice, the FI would find itself in the unenviable position of having to procure legal opinions from each and every jurisdiction that the cloud service provider operates from, and to "regularly update" its legal advice, before adopting a cloud solution involving the hosting of data in those jurisdictions. The prohibitive costs of compliance would likely render a cloud service untenable as cloud service providers typically operate out of numerous jurisdictions.

There is uncertainty as to how "regularly" the legal advice must be updated, as well as the required scope of the legal advice. From the legal perspective, it is also questionable whether it is possible to set out exhaustively all scenarios in which customer information may potentially be disclosed notwithstanding an obligation of confidentiality.

Further, FIs will face difficulties communicating to their customers the risks of disclosure of customer information in each jurisdiction, and there is ambiguity as to the scope of communication to the FI's customers, that is, how much information the FI is required to disclose to its customers in order to comply. Feedback #1 applies here: The requirements in paragraph 6.3 are simply not measureable and should not be included in the Notice.

It should also be noted that the Personal Data Protection Act 2012 (PDPA) has come into force. Understandably, the kind of data protected by the PDPA is narrower than the data sought to be protected under the proposed Guidelines and Notice. However, in principle, the types of data protected by the two regimes are not too different from each other that they warrant two different risk management regimes. The above is not required under the PDPA. To contain risk management and compliance costs, harmonization of the two regimes would be desirable.

Request #3: To remove paragraph 9.1 of the proposed Notice.

Reference:

Proposed Notice, paragraph 9.1

"9.1 Where the service provider is an overseas regulated financial institution, an institution required by any law or regulation administered by the Authority to protect or not to disclose customer information shall give the Authority a written confirmation by the supervisory authority of the service provider to the effect that:

(a) the Authority and any independent auditors appointed by the Authority shall be allowed access by the supervisory authority to the institution's documents, records of transactions, information previously given to, stored or processed by the service provider;

(b) the institution and any auditor appointed by the institution shall not be inhibited from inspecting the control environment within the service provider insofar as it relates to the institution's data that is processed by the service provider, or from reporting any findings to the Authority;

(c) in the case where the supervisory authority is a host supervisor of the overseas regulated financial institution, it shall not access any customer information of the Singapore office that is in the possession of the overseas regulated financial institution ("the Information");

(d) in the case where the supervisory authority is the home supervisor of the overseas regulated financial institution:

(i) it shall not access the Information unless access to the Information is required for the sole purpose of carrying out its supervisory functions;

(ii) it shall give the Authority prior written notification whenever it accesses the Information; and

(e) *it is prohibited under its laws from disclosing the Information to any other person, or it undertakes to safeguard the confidentiality of the Information and not disclose the Information to any other person."*

Comments:

We understand that in practice, FIs would face difficulties obtaining such written confirmation from overseas regulators – even where intra-group outsourcing is concerned. It would be more appropriate for MAS to approach the overseas regulators directly to come to an agreed arrangement or treaty, or in the alternative, for MAS to waive the requirement for such written confirmation to be obtained in certain circumstances, such as where intra-group outsourcing is concerned.

FEEDBACK #3

The Notice must not assume that service providers and their sub-contractors will always be ready, willing and able to contractually agree to the "minimum standards".

The proposed Notice appears to have been drafted on the implicit assumption that service providers and their sub-contractors will be ready, willing and able to contractually agree to the requirements in the Notice.

However, the commercial reality is that service providers can, and do, push back on these requirements, and may decide not to contract with an FI if negotiations break down. Further, cloud service providers typically do not have full control over their sub-contractors and, more often than not, do not have the bargaining power to extract the rights necessary to enable FIs to comply.

Request #1: Provisions that require the service provider and their sub-contractors to agree to should not be put in a Notice. MAS can suggest model clauses for inclusion in agreements in the Guidelines.

Reference:

Proposed Notice, paragraph 8.1

"8.1 An institution shall include in all its outsourcing agreements a right to terminate the outsourcing agreement in the event that:

(a) the service provider undergoes a change in ownership, becomes insolvent, goes into liquidation, receivership or judicial management;

(b) there has been a breach of confidentiality by the service provider or its sub-contractors that affect the institution or the institution's customers;

(c) there has been a deterioration in the ability of the service provider to perform the service as contracted;

(d) the institution is prevented from conducting any audits or obtaining any report and finding made on the service provider;

(e) the institution is prevented from assessing the service provider's compliance with the outsourcing agreement; or

(f) the institution is directed by the Authority to terminate the outsourcing arrangement as the service provider has failed to comply with all applicable laws and regulations."

Comments: The commercial reality is that, subject to the bargaining position between the FI and the service provider, the service provider typically would not agree to these provisions, for example, a right to terminate for any change in ownership, or any breach of confidentiality (even if trivial).

There is also ambiguity in the wording used in paragraph 8.1(c) as it is not clear what "deterioration" means. As a result, there is uncertainty as to what FIs need to include in their outsourcing agreements in order to comply. MAS should therefore propose model clauses for inclusion in the outsourcing agreements. These should be placed in the Guidelines and not in the Notice, as it should not be assumed that service providers will agree to such provisions.

Request #2: To remove paragraph 5.5.2(j) of the proposed Guidelines.

Reference:

Proposed Guidelines, paragraph 5.5.2(j)

"*The institution should ensure that sub-contracting of material outsourcing arrangements should be subject to prior approval of the institution*." [Emphasis added]

Comments:

Prior approval by FIs should not be necessary for sub-contracting of material outsourcing arrangements unless all or substantially all of the service provided is sub-contracted.

Cloud service providers often engage a large number of sub-contractors to provide components of services and/or solutions to various customers. The above requirement will mean that cloud service providers will potentially be required to secure the prior approval of each and every customer that is a regulated FI, prior to engaging a particular sub-contractor to service all of those customers. This is simply not practical and does not accord with industry practice.

Request #3: FIs' due diligence obligations should not extend to the service provider's sub-contractors, and employees of the service provider and its sub-contractors. Further, FIs should not be expected to carry out independent audits and expert assessments of the service provider's sub-contractors.

Reference:

Proposed Guidelines, paragraph 5.3.1(c)

"*The institution should establish a framework for risk evaluation which should include… assessment of the service provider and its sub-contractors in the outsourcing arrangement, and their ability to employ the high standard of care and meet the regulatory standards as expected of the institution, and comply with applicable laws and regulations, as if the outsourcing arrangement were being conducted by the institution…*" [Emphasis added]

Proposed Guidelines, paragraph 5.9.5

"*An institution should ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the institution should consider the nature and extent of risk and impact to the institution from the outsourcing arrangements. The period between audits should not exceed 3 years. The scope of the audits and expert assessments should include an assessment of the service providers' and its sub-contractors' security and control environment, incident management process (for material breaches, service disruptions or other material issues) and the institution's observance with MAS' Guidelines on Outsourcing and compliance with the Notice on Outsourcing in relation to the outsourcing arrangement.*" [Emphasis added]

Proposed Guidelines, paragraph 5.4.4

"The institution should ensure that the employees of the service provider and its sub-contractors undertaking any part of the outsourcing arrangement have been assessed to be fit and proper, consistent with the criteria applicable to its own employees. The following are some non-exhaustive examples of what could be considered under the fit and proper assessment:

(a) whether they have been the subject of any proceedings of a disciplinary or criminal nature;
(b) whether they have been convicted of any offence (in particular, that associated with a finding of fraud, misrepresentation or dishonesty);
(c) whether they have accepted civil liability for fraud or misrepresentation; and
(d) whether they are financially sound. ..."

Comments:

Due to the large number of sub-contractors normally involved for supply of cloud computing services, for both FIs and service providers, expansion of the scope of the institution's due diligence obligation would likely mean an exponential increase in due diligence costs. It may not make business sense for cloud service providers to offer shared resources to FIs when each shared sub-contractor could potentially be subject to at least as many due diligence exercises as the number of unique customers they intend to service.

Bird & Bird

FEEDBACK #4

FIs should not be required to include in their outsourcing agreements indemnity clauses that hold MAS harmless.

Request: To remove the requirement for indemnity clauses to be included in the outsourcing agreements between FIs and their service providers.

Reference:

Proposed Notice, paragraph 5.1(c)

"*An institution shall include in all its outsourcing agreements provisions that: ... indemnify and hold the Authority, its officers, agents and employees harmless from any liability, loss or damage to the service provider and its sub-contractors arising out of any action taken to access and inspect the service provider or its sub-contractors pursuant to the outsourcing agreement.*"

Proposed Guidelines, paragraph 5.9.2

"*An institution should include in all its outsourcing agreements clauses that: ... indemnify and hold MAS, its officers, agents and employees harmless from any liability, loss or damage to the service provider and its sub-contractors arising out of any action taken to access and inspect the service provider or its sub-contractors pursuant to the outsourcing agreement.*"

Comments:

It appears from the wording of the proposed Guidelines and Notice that the indemnity is intended to be broad in scope, and not subject to any limitations or exclusions of liability. It is of great concern to both FIs and service providers that the indemnity has been stated so broadly.

Bird & Bird

Where MAS has acted in good faith, MAS is entitled to rely on the "good faith" immunity under section 22 of the Monetary Authority of Singapore Act. Where MAS has failed to act in good faith, for example where there is fraud, it is difficult to understand why MAS should be indemnified.

It is not clear why there is a need to require such an indemnity in the outsourcing agreement where the agreement is between the FIs and the service provider. MAS should provide clarification on its objectives in seeking a blanket indemnity to be included in the outsourcing agreement.

FEEDBACK #5

To protect the confidentiality of customer information, it is not necessary to require the service provider to isolate and clearly identify the FIs' customer information

Request: To remove paragraph 6.2 of the proposed Notice.

Reference:

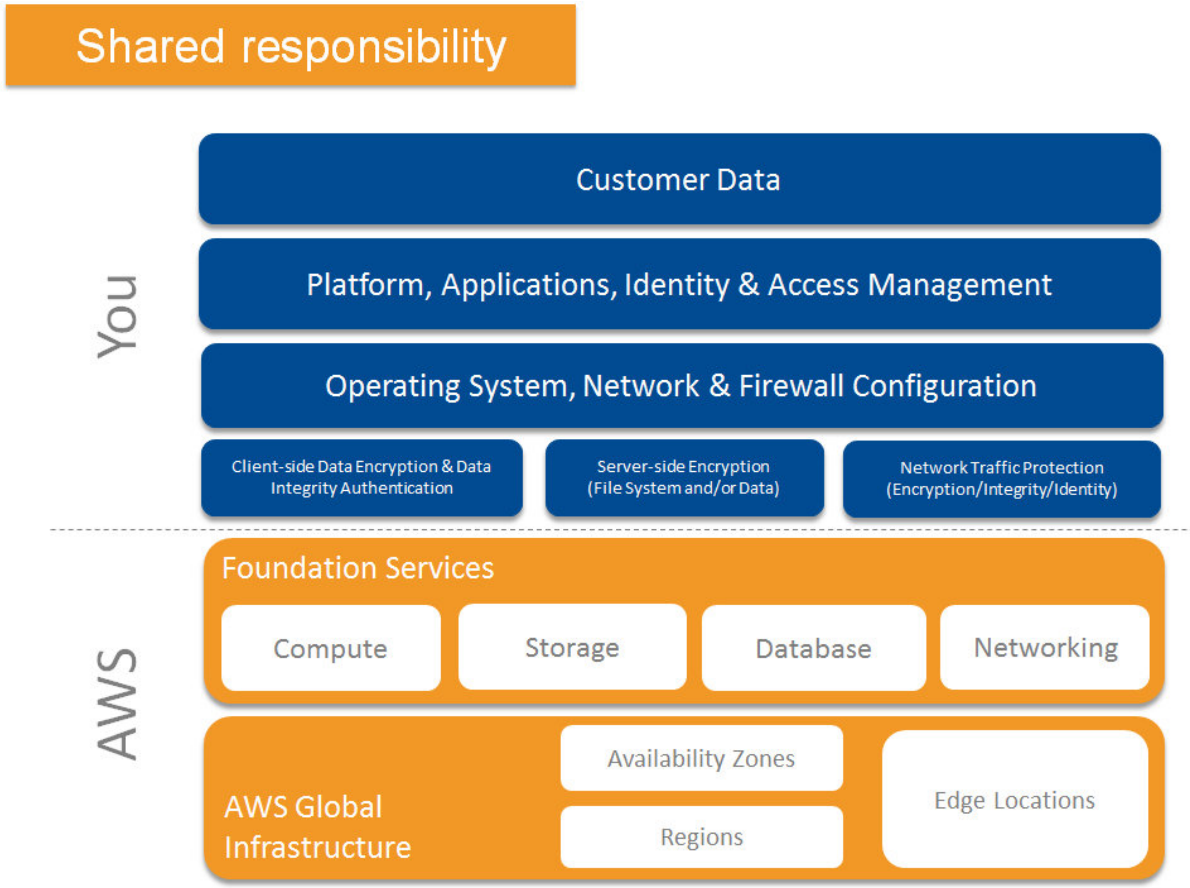
Proposed Notice, paragraph 6.2

"An institution shall require the service provider to isolate and clearly identify the institution's customer information, documents, records, and assets to protect the confidentiality of the information."

Comments:

Feedback #2 and Feedback #3 apply equally here. Firstly, this provision assumes that the service provider is always responsible for confidentiality, integrity and availability of customer data, which is not always the case.

For example, the figure below from Amazon Web Services (AWS) Privacy whitepapers, available at aws.amazon.com/compliance, illustrates a technology outsourcing arrangement where the customer is responsible for the integrity and confidentiality of the customer's data, while AWS merely provides the back-end infrastructure and foundation services. In such a scenario, it would not make sense for the service provider, in this case AWS, to agree to isolate and identify the FI's customer information, documents and records:-



Further, the above provision in the proposed Notice also assumes that data can be isolated and identified at all times. However, a cloud or shared service platform, infrastructure and/or application may contain information from various customers, and we understand that from a technical or operational perspective, it may not be possible always to isolate and clearly identify the FIs' customer information at all times, such as when data flow is taking place, or is in transit, or enters a node where activities are logged, or where there are multiple sub-sub-contractors.

In any case, information of FIs put together in a secured environment will remain confidential notwithstanding they are not separated at all times.

Bird & Bird

CONCLUDING REMARKS

Based on the above, it is likely that if the proposed Guidelines and Notice are adopted, both FIs and their service providers could face immense practical and operational difficulties with compliance, as well as substantial costs of compliance that may far outweigh the commercial benefits typically associated with cloud services.

It is a real and foreseeable danger that cloud service providers may simply exit the market in search of business in other jurisdictions, and FIs subject to the proposed Guidelines and Notice may find themselves stranded with few or no service providers who are willing or able to do business here – resulting in a vicious cycle that makes it increasingly difficult for FIs to comply with the proposed Guidelines and Notice particularly where technology outsourcing is concerned. An industry-wide business impact analysis should be carried out before implementing the Guidelines and Notice.

It is therefore hoped that MAS will revise the proposed Guidelines and Notice so as to encourage proper risk management practices without unduly stifling the adoption of technology by regulated FIs.

twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Skanderborg & Stockholm & Warsaw

Bird & Bird

CONTACTS

KOH, Chia Ling

Partner, ATMD Bird & Bird LLP

Advocate & Solicitor, Singapore

MTech (KE), CISSP

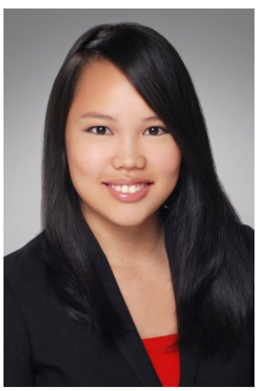
D: +65 64289452
T: +65 65435266
chialing.koh@twobirds.com

Marcus Chow

Partner, ATMD Bird & Bird LLP

Advocate & Solicitor, Singapore

D: +65 64289425
T: +65 65435266
marcus.chow@twobirds.com



Angelique CHAN

Associate, ATMD Bird & Bird LLP

Advocate & Solicitor, Singapore

D: +65 64289840
T: +65 65435266
angelique.chan@twobirds.com

twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Skanderborg & Stockholm & Warsaw