Water Dragon Solutions Pte Ltd,
the Compliance Practice of
Maroon Analytics
63 Robinson Road
#04-04 Afro Asia Building
Singapore 068894
+65 8192 1784

www.maroonanalytics.com

MAROON

your edge on complexity

Regulatory Update
September 2016

MAS Guidelines on Outsourcing

Overview

Jurisdiction	Singapore
Executive Summary	The Monetary Authority of Singapore ("MAS") has issued amended Guidelines on Outsourcing Risk Management ("Outsourcing Guidelines") to financial institutions ("FIs"). The several key changes to the Guidelines in the revision are: • The definition of "material outsourcing arrangement" has been revised to include an arrangement that involves customer information. • The expectation for FIs to pre-notify MAS of material outsourcing arrangements has been removed. • A new section on cloud computing has been incorporated that submits cloud computing to the Outsourcing Guidelines (and thus confirms that FIs can make use of it).
Effective Date	Immediate

The New Rules

MAS Guidelines on Outsourcing

The MAS has issued amended Guidelines on Outsourcing Risk Management to FIs. The revised guidelines provide guidance on sound risk management practices for outsourcing and build on the existing guidelines, in order to better capture evolving threats such as offshore business models and increased cyber risks. The revised guidelines take into account new practices adopted by FIs such as the use of cloud services and provide guidance on how to mitigate the new risks. The revised guidelines replace the existing Outsourcing Guidelines as well as the circular on Information Technology Outsourcing.

MAS will review the implementation of the Outsourcing Guidelines by an FI to assess the quality of its board and senior management oversight and governance, internal controls and risk management. In particular, MAS will be focusing its attention on material outsourcing arrangements.

Material Outsourcing Arrangements

MAS has revised the definition of "material outsourcing arrangement" under the new Outsourcing Guidelines to include, under certain circumstances, an arrangement that involves customer information. A "material outsourcing arrangement" refers to an outsourcing arrangement (a) which, in the event of a service failure or security breach, has the potential to either materially impact an institution's (i) business operations, reputation or profitability or (ii) ability to manage risk and comply with applicable laws and regulations, or (b) which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on an institution's customers.

MAS has also removed the expectation for FIs to pre-notify MAS before making any material outsourcing commitment.

Engagement with MAS on Outsourcing

Instead of the pre-notification of material outsourcing arrangements, FIs are expected to exercise the appropriate due diligence on their outsourcing arrangements. FIs must be prepared to demonstrate to the MAS their adherence to the Outsourcing Guidelines. Under the Outsourcing Guidelines, FIs should submit the outsourcing register to MAS at least on an annual basis or upon request. An FI should submit its outsourcing register to MAS using the template provided in Annex 3 of the Outsourcing Guidelines. However, FIs are allowed to use a different template to update its board and senior management of its outsourcing arrangements.

The FI must also notify MAS as soon as possible of any adverse development arising from its outsourcing arrangements that could impact the FI. This includes any event that could lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the FI's customer information. An FI should also notify MAS of such adverse developments encountered within the its group.

FIs will be required to take additional measures to address deficiencies where MAS is not satisfied with the FI's observance of the Outsourcing Guidelines. Such non-compliance may be taken into account during MAS's assessment of the FI, and is dependent on factors such as the potential impact of the outsourcing on the FI and the financial system, seriousness of the deficiencies and the FI's track record in internal

controls and risk management. MAS may require an FI to modify, make alternative arrangements or re-integrate an outsourced service where the FI fails to demonstrate an adequate level of understanding of the nature and risks arising from the outsourcing arrangement as well as implement adequate measures to address those risks.

Risk Management Practices

Responsibility of the Board and Senior Management

The board and senior management of the FI are ultimately responsible for maintaining effective oversight and governance of outsourcing arrangements, managing outsourcing risks, and implementing an adequate outsourcing risk management framework, in accordance with the Guidelines. The board and senior management of an FI must ensure there are adequate processes to provide a comprehensive understanding of the FI's risk exposures from outsourcing, and incorporate the assessment and mitigation of such risks into its outsourcing risk management framework.

The board, or a committee delegated by it, is responsible for:

a) approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the applicable policies that apply;
b) setting a suitable risk appetite to define the nature and extent of risks that the institution is willing and able to assume from its outsourcing arrangements;
c) laying down appropriate approval authorities for outsourcing arrangements consistent with its established strategy and risk appetite;
d) assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements;
e) ensuring that senior management establishes appropriate governance structures and processes for sound and prudent risk management; and
f) undertaking regular reviews of these outsourcing strategies and arrangements for their continued relevance, and safety and soundness.

Senior management is responsible for:

a) evaluating the materiality and risks from all existing and prospective outsourcing arrangements, based on the framework approved by the board;
b) developing sound and prudent outsourcing policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements as well as ensuring that such policies and procedures are implemented effectively;
c) reviewing regularly the effectiveness of, and appropriately adjusting, policies, standards and procedures to reflect changes in the FI’s overall risk profile and risk environment;
d) monitoring and maintaining effective control of all risks from its material outsourcing arrangements on an institution-wide basis;
e) ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested;
f) ensuring that there is independent review and audit for compliance with outsourcing policies and procedures;
g) ensuring that appropriate and timely remedial actions are taken to address audit findings; and
h) communicating information pertaining to risks arising from its material outsourcing arrangements to the board in a timely manner.

For an FI established outside Singapore, the functions of the board may be delegated to and performed by a management committee or body beyond local management that is charged to functionally oversee and supervise the local office. The local management of an FI established outside Singapore should continue to take the necessary steps to enable it to discharge its obligations to comply with the relevant laws and regulations in Singapore, including expectations under the Guidelines.

The board should establish communication procedures between the board and the committee where it delegates its responsibility to a committee. The committee should report to the board regularly and the board must ensure that senior management is held responsible for the implementation of the guidelines. However, it should be noted that ultimately the board is responsible for the performance of its responsibilities by that committee.

Evaluation of Risks

The FI must establish a framework for risk evaluation of the risks arising from outsourcing. Risk evaluations should be performed when an FI is planning to enter into an outsourcing arrangement with an existing or a new service provider, and also re-performed periodically on existing outsourcing arrangements.

The institution should establish a framework for risk evaluation which:

a) identifies the role of outsourcing in the overall business strategy and objectives of the institution;
b) performs comprehensive due diligence on the nature, scope and complexity of the outsourcing arrangement to identify and mitigate key risks;
c) assesses the service provider's ability to employ a high standard of care in performing the outsourced service and meet regulatory standards;
d) analyses the impact of the outsourcing arrangement on the overall risk profile of the FI, and whether there are adequate internal expertise and resources to mitigate the risks identified;
e) analyses the FI's as well as its group aggregate exposure to the outsourcing arrangement, to manage concentration risk; and
f) analyses the benefits of outsourcing against the risks that may arise, ranging from the impact of temporary disruption to service to that of a breach in security and confidentiality.

Assessment of Service Providers

The FI should subject the service provider to appropriate due diligence processes to assess the risks associated with outsourcing arrangements. The FI must assess the service provider's capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the FI to meet its obligations as a regulated entity. The due diligence must take into account the physical and IT security controls of the service provider, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, as well as the ability of the service provider to meet obligations under the outsourcing arrangement. Onsite visits conducted by persons possessing the requisite knowledge and skills should be performed as part of the assessment of the service provider. The FI should also assess the employees of the service provider to ensure they meet the FI's hiring policies and that they are consistent with the criteria applicable to its own employees. Due diligence undertaken during the assessment process should be documented and re-performed periodically and the FI should ensure that the information used for the due diligence evaluation is sufficiently current.

Outsourcing Agreement

Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement should be carefully and properly defined in written agreements. They should also be vetted by a competent authority on their legality and enforceability.

The FI should ensure that every outsourcing agreement addresses the risks identified at the risk evaluation and due diligence stages. Each outsourcing agreement should allow for timely renegotiation and renewal to enable the institution to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations. It should have provisions to address the following aspects of outsourcing:

a) scope of the outsourcing arrangement;
b) performance, operational, internal control and risk management standards;
c) confidentiality and security;
d) business continuity management;
e) monitoring and control;
f) audit and inspection;
g) notification of adverse developments;
h) dispute resolution;
i) default termination and early exit;
j) sub-contracting;
k) applicable laws.

Confidentiality and Security

The FI must ensure that the service provider has proper security policies, procedures and controls in place in order to protect the confidentiality and security of the FI's customer information. The FI must take the initiative to identify and specify the requirements for confidentiality and security in the outsourcing arrangement. The FI should take these necessary steps to protect the confidentiality and security of customer information:

a) State the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices;
b) Disclose customer information to the service provider only on a need-to-know basis;
c) Ensure the service provider is able to protect the confidentiality of customer information, documents, records, and assets;
d) Review and monitor the security practices and control processes of the service provider on a regular basis.

Business Continuity Management

The FI must adopt the sound practices and standards as stated in the MAS Business Continuity Management ("BCM") Guidelines, when assessing the impact of outsourcing on its risk profile. The FI must take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated such that the FI is still able to conduct its business with integrity and competence in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the service provider. These should include taking the following steps:

a) Determine that the service provider has in place satisfactory business continuity plans ("BCP") that are commensurate with the nature, scope and complexity of the outsourcing arrangement. Outsourcing agreements should contain BCP requirements on the service provider, in particular, recovery time objectives ("RTO"), recovery point objectives ("RPO"), and resumption operating capacities;
b) Proactively seek assurance on the state of BCP preparedness of the service provider, or participate in joint testing, where possible. It should ensure the service provider regularly tests its BCP plans and that the tests validate the feasibility of the RTO, RPO and resumption operating capacities; and
c) Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the institution will be able to continue business operations and that all documents, records of transactions and information previously given to the service provider should be promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable.

The FI should design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement. The FI should cooperate with the service provider in the validation of its BCP and assessment of the awareness and preparedness of its own staff and take part in the service providers' BCP and disaster recovery exercises. In addition, the FI should consider worst case scenarios in its business continuity plans.

Monitoring and Control of Outsourcing Arrangements

An FI should establish a structure for the management and control of its outsourcing arrangements. Where relationships and interdependencies with regards to outsourcing arrangements increase in materiality and complexity, the FI should adopt a more rigorous risk management approach. The FI should ensure that it has frequent communication with the service provider and this can be done through having regular meetings. This is to ensure that performance, operational, internal control and risk management standards remains up to standard. In addition, the FI should ensure that outsourcing agreements with service providers contain clauses to address the institution's monitoring and control of outsourcing arrangements.

Several measures can be put in place for FIs to effectively monitoring and control its material outsourcing arrangements:

a) The FI should maintain a register of all material outsourcing arrangements and ensure that the register is accessible for review by its board and senior management. Information maintained in the register should include those set out in Annex 3 of the Guidelines. The register should be updated promptly and form part of the reviews undertaken by the board and senior management;
b) The FI should establish multi-disciplinary outsourcing management groups with members from different risk and internal control functions including legal, compliance and finance, to ensure that all relevant technical issues and legal and regulatory requirements are met;
c) The FI should establish outsourcing management control groups to monitor and control the outsourced service on an ongoing basis. Policies and procedures should be in place to monitor service delivery and the confidentiality and security of customer information;
d) The FI should perform reviews at least on an annual basis on all material outsourcing arrangements to ensure that the FI's outsourcing risk management

policies and procedures and the Outsourcing Guidelines are effectively implemented;

e) Reports on the monitoring and control activities of the FI should be reviewed by senior management and provided to the board. When adverse development occurs, prompt action should be taken by the FI to review the outsourcing relationship for modification or termination of the agreement;
f) The FI should also perform comprehensive pre- and post- implementation reviews of new outsourcing arrangements or when amendments are made to the outsourcing arrangements. If an outsourcing arrangement is materially amended, a comprehensive due diligence of the outsourcing arrangement should also be conducted.

Audit and Inspection

The FI's outsourcing arrangements should not interfere with the ability of the FI to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives. The FI should include, in all its outsourcing agreements for material outsourcing arrangements, clauses that:

a) allow the FI to conduct audits on the service provider and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the FI; 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;
b) allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the FI to:
    i. access and inspect the service provider and its sub-contractors, and obtain records and documents, of transactions, and information of the FI given to, stored at or processed by the service provider and its sub-contractors;
    ii. 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.

Outsourcing agreements for material outsourcing arrangements should also include clauses requiring the service provider to comply with any request from MAS or the FI, to the service provider or its sub-contractors, to submit any reports on the security and control environment of the service provider and its sub-contractors to MAS, in relation to the outsourcing arrangement.

The FI must ensure that these expectations are met in its outsourcing arrangements with the service provider as well as any sub-contractor that the service provider may engage in the outsourcing arrangement, including any disaster recovery and backup service providers. MAS will provide the FI reasonable notice of its intent to exercise its inspection rights and share its findings with the FI where appropriate. The FI should also ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted. The independent audit and/or expert assessment on the service provider and its sub-contractors may be performed by the FI's internal or external auditors, the service provider's external auditors or by agents appointed by the FI. The appointed persons should possess the requisite knowledge and skills to perform the engagement, and be independent of the unit or function performing the outsourcing arrangement.

Senior management should ensure that appropriate and timely remedial actions are taken to address the audit findings. FIs and the service providers should have adequate

processes in place to ensure that remedial actions are satisfactorily completed. Actions taken by the service provider to address the audit findings should be appropriately validated by the FI before closure. Where necessary, the relevant persons who possess the requisite knowledge and skills should be involved to validate the effectiveness of the security and control measures taken.

Significant issues and concerns should be brought to the attention of the board and senior management of the FI and service provider on a timely basis. Actions should be taken by the FI to review the outsourcing arrangement if the risk posed is no longer within the FI's risk tolerance. Copies of audit reports should be submitted to MAS. The FI should also upon request provide MAS with other reports or information on the FI and service provider that is related to the outsourcing arrangement.

Outsourcing Outside Singapore

The FI must be aware that the engagement of a service provider in a foreign country, or an outsourcing arrangement whereby the outsourced function is performed in a foreign country, may expose the FI to country risk that may adversely affect the FI. The FI should take into account the government policies; political, social, economic conditions; legal and regulatory developments in the foreign country and the institution's ability to effectively monitor the service provider and execute its business continuity management plans and exit strategy. The FI should also be aware of the disaster recovery arrangements and locations established by the service provider. Material outsourcing arrangements with service providers located outside Singapore should be conducted in such a way that it does not hinder MAS' efforts to supervise the Singapore business activities of the FI in a timely manner.

The FI should enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements. The FI should not enter into outsourcing arrangements with service providers in jurisdictions where prompt access to information by MAS or agents appointed by MAS to act on its behalf, at the service provider, may be impeded by legal or administrative restrictions.

The FI must at least commit to retrieve information readily from the service provider should MAS request for such information. The FI should confirm in writing to MAS, that it has provided, in its outsourcing agreements, for MAS to have the rights of inspecting the service provider, as well as the rights of access to the institution and service provider's information, reports and findings related to the outsourcing arrangement. The FI should notify MAS if any overseas authority were to seek access to its customer information or if a situation arises where the rights of access of the FI and MAS, have been restricted or denied.

Outsourcing Within a Group

It should be noted that the Outsourcing Guidelines are applicable to outsourcing arrangements with parties within an institution's group and may be addressed within group-wide risk management policies and procedures. The FI is expected to provide, when requested, information demonstrating the structure and processes by which its board and senior management discharge their role in the oversight and management of outsourcing risks on a group-wide basis. Due diligence on an intra-group service provider may be in the form of assessing the qualitative aspects of the service provider's ability to address risks specific to the FI, in particular, for those relating to business continuity management, monitoring and control, audit and inspection, confirmation on the right of access to be provided to MAS, to retain effective supervision over the institution, and compliance with local regulatory standards. The

respective roles and responsibilities of each office in the outsourcing arrangement must be documented in writing such as in a service level agreement.

Outsourcing of Internal Audit to External Auditors

One issue that needs to be addressed is the perceived lack of independence or impaired independence when a service provider is handling multiple engagements for an FI such as internal and external audits and consulting work. As a sound practice, FIs should not outsource their internal audit function to the institution's external audit firm. Before outsourcing the internal audit function to external auditors, the FI should satisfy itself that the external auditor would be in compliance with the relevant auditor independence standards of the Singapore accounting profession.

Cloud Computing

MAS has incorporated a new section on cloud computing into the revised Outsourcing Guidelines. Cloud services ("CS") are a combination of a business and delivery model that enable on-demand access to a shared pool of resources such as applications, servers, storage and network security. The service is usually delivered in the form of Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

CS deployments can be operated in-house or off-premises by service providers. CS operated off-premises can take the form of a private or public cloud, however there is increasing evidence which indicate that FIs are adopting a combination of private and public clouds to create a hybrid cloud. The different cloud models provide for distinct operational and security trade-offs.

As evident in recent years, cloud technology has evolved and matured considerably and CS providers have become aware of the technology and security requirements of FIs to protect sensitive customer data. CS providers in general, have implemented strong authentication, access controls, tokenisation techniques and data encryption to bolster security to meet requirements of FIs. MAS considers CS operated by service providers as a form of outsourcing and recognises that FIs may leverage on such a service to enhance their operations and service efficiency while reaping the benefits of CS' scalable, standardised and secured infrastructure. FIs must perform the necessary due diligence and apply sound governance and risk management practices as set out in the Outsourcing Guidelines.

FIs must take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. They must ensure that the service provider possesses the ability to clearly identify and segregate customer data using strong physical or logical controls. The service provider should have in place robust access controls to protect customer information and such access controls should survive the tenure of the contract of the CS. FIs are ultimately responsible and accountable for maintaining oversight of CS and managing the attendant risks of adopting CS, as in any other form of outsourcing arrangements. A risk-based approach should be taken by FIs to ensure that the level of oversight and controls are commensurate with the risks posed by the CS.

For more information or further discussions, please contact Water Dragon Solutions Pte Ltd, the Compliance Practice of Maroon Analytics Pte Ltd: **compliance@maroonanalytics.com.**