Monetary Authority of Singapore

GUIDELINES ON OUTSOURCING

27 July 2016

[Last revised on 5 October 2018
(with effect from 8 October 2018)]

Table of Contents

1 INTRODUCTION

1.1 While outsourcing arrangements can bring cost and other benefits, it may increase the risk profile of an institution due to, for example, reputation, compliance and operational risks arising from failure of a service provider in providing the service, breaches in security, or the institution's inability to comply with legal and regulatory requirements. An institution can also be exposed to country risk when a service provider is located overseas and concentration risk when more than one function is outsourced to the same service provider. Outsourcing does not diminish the obligations of an institution, and those of its board and senior management to comply with relevant laws and regulations in Singapore, it is thus important that an institution adopts a sound and responsive risk management framework for its outsourcing arrangements.

1.2 These Guidelines[1] on Outsourcing ("Guidelines") set out the Monetary Authority of Singapore's ("MAS") expectations of an institution that has entered into any outsourcing arrangement or is planning to outsource its business activities[2] to a service provider. An institution should conduct a self-assessment of all existing outsourcing arrangements against these Guidelines[3].

2 APPLICATION OF GUIDELINES

2.1 These Guidelines provide guidance on sound practices on risk management of outsourcing arrangements. The Guidelines do not affect, and should not be regarded as a statement of the standard of care owed by institutions to their customers. The extent and degree to which an institution implements the Guidelines should be commensurate with the nature of risks in, and materiality of, the outsourcing arrangement. An institution should ensure that outsourced services (whether provided by a service provider or its sub-contractor) continue to be managed as if the services were still managed by the institution. In supervising an institution, MAS will review the implementation of these Guidelines by an institution to assess the quality of its board and senior management oversight and governance, internal controls and risk management. MAS is particularly interested in material outsourcing arrangements.

[1] Please refer to MAS' website (www.mas.gov.sg) for details of the classification of instruments issued by MAS.

[2] Any reference in these Guidelines to "business activities" of an institution is to be construed as a reference to the business and operational functions and processes of the institution.

[3] This includes institutions which are bound by outsourcing arrangements as a result of an acquisition of the business of another institution.

2.2 Annex 1 provides a non-exhaustive list of examples of outsourcing arrangements to which these Guidelines are applicable, and arrangements that are not intended to be subject to these Guidelines. It should also not be misconstrued that arrangements not defined as outsourcing need not be subject to adequate risk management and sound internal controls. Annex 2 provides guidance to an institution in assessing whether an arrangement would be considered a material outsourcing arrangement. Annex 3 provides a template for an institution to maintain a register of its outsourcing arrangements which is to be submitted to MAS, at least annually or upon request.

2.3 An institution incorporated in Singapore should also consider the impact of outsourcing arrangements by its branches and any corporation under its control, including those located outside Singapore, on its consolidated operations. Institutions incorporated in Singapore should ensure that these Guidelines are observed by branches and corporations under their control by applying a group-wide outsourcing risk management framework that complies with the Guidelines.

2.4 The practices articulated in these Guidelines are not intended to be exhaustive or override any legislative provisions. They should be read in conjunction with the provisions of the relevant legislation, the subsidiary legislation made under the relevant legislation, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

3 DEFINITIONS

3.1 In these Guidelines on Outsourcing, unless the context otherwise requires:

"benchmark administrator" means a benchmark administrator authorised under section 123F of the Securities and Futures Act (Cap. 289) ("SFA") or a benchmark administrator exempt under section 123K of the SFA;

"board" or "board of directors" means –

(a) in the case of an institution incorporated in Singapore, the board of directors; and

(b) in the case of an institution incorporated or established outside Singapore, a management committee or body beyond local management charged with oversight and supervision responsibilities for the institution in Singapore;

"bridge-institution" means an institution, whether incorporated in Singapore or outside Singapore, to temporarily take over and maintain certain assets, liabilities and operations of a distressed financial institution, as part of a resolution Authority's exercise of a resolution power;

"business relations" –

(a) in relation to an insurer, means
  (i) the issuance of a policy or reinsurance cover by the insurer to; or
  (ii) the provision of financial advice by the insurer to,
  a person (whether a natural person, legal person or legal arrangement);

(b) in relation to a bank, means
  (i) the opening or maintenance of an account by the bank in the name of; or
  (ii) the provision of financial advice by the bank to,
  a person (whether a natural person, legal person or legal arrangement);

(c) in relation to a CMI, means
  (i) the opening or maintenance of an account by the CMI in the name of;
  (ii) the provision of financial advice by the CMI to; or
  (iii) the provision of fund management services by the CMI to,
  a person (whether a natural person, legal person or legal arrangement);

(d) in relation to a financial adviser, means

(i) the opening or maintenance of an account by the financial adviser in the name of; or

(ii) the provision of financial advice by the financial adviser to,

a person (whether a natural person, legal person or legal arrangement);

(e) in relation to a credit card or charge card licensee licensed under section 57B of the Banking Act (Cap. 19), means the opening or maintenance of an account by the credit card or charge card licensee in the name of a person (whether a natural person, legal person or legal arrangement);

(f) in relation to a benchmark administrator, means

(i) the collection of information from a person (whether a natural person, legal person or legal arrangement) by the benchmark administrator for the purpose of administering a designated benchmark under the SFA; or

(ii) the provision of a designated benchmark by the benchmark administrator to, a person (whether a natural person, legal person or legal arrangement);

"CMI" means a person holding a capital markets services licence under the SFA, a fund management company registered under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations ("SF(LCB)R") or a person exempted from the requirement to hold such a licence under paragraph 7(1)(b) of the Second Schedule to the SF(LCB)R;

"customer" means –

(a) in relation to any trustee for a collective investment scheme authorised under section 286 of the SFA, that is approved under that Act, the managers and participants of the collective investment scheme;

(b) in relation to an approved exchange, recognised market operator, licensed trade repository, licensed foreign trade repository, approved clearing house, recognised clearing house, and central depository system under the SFA, a person who may participate in one or more of the services provided by such entities;

(c) in relation to a licensed trust company under the Trust Companies Act (Cap. 336), a trust for which the trust company provides trust business services and includes the settlor and any beneficiary under the trust;

(d) in relation to a bank, means a person (whether a natural person, legal person or legal arrangement) −

(i) with whom the bank establishes or intends to establish business relations; or

(ii) for whom the bank undertakes or intends to undertake any transaction without an account being opened;

(e) in relation to an insurer, means a person (whether a natural person, legal person or legal arrangement) with whom the insurer establishes or intends to establish business relations, including, in the case of a group policy, the owner of the master policy issued or intended to be issued;

(f) in relation to an insurance intermediary, means a person (whether a natural person, legal person or a legal arrangement) with whom the insurance intermediary arranges or intends to arrange for such persons, contracts of insurance in Singapore with one or more insurers;

(g) in relation to a financial adviser, means a person (whether a natural person, legal person or a legal arrangement) with whom the financial adviser establishes or intends to establish business relations and includes in the case where the financial adviser arranges a group life insurance policy, the owner of the master policy;

(h) in relation to a CMI, means a person (whether a natural person, legal person or a legal arrangement) –

(i) with whom the CMI establishes or intends to establish business relations;

(ii) for whom the CMI undertakes or intends to undertake any transaction without an account being opened; or

(iii) who invests into an investment vehicle to which the CMI provides the regulated activities of fund management and real estate investment trust management;

(i) in relation to a credit card or charge card licensee licensed under section 57B of the Banking Act (Cap. 19), means a person (whether a natural person, legal person or legal arrangement) with whom the credit card or charge card licensee establishes or intends to establish business relations;

(j) in relation to money-changers and remittance businesses, means a person (whether a natural, legal person or legal arrangement) –

(i) with whom the licensee establishes or intends to establish an account relationship; or

(ii) for whom the licensee undertakes or intends to undertake a relevant business transaction without an account being opened, including in the case of an inward remittance transaction, the person to whom the licensee pays out funds in cash or cash equivalent in Singapore and the person on behalf of whom such funds are paid out in Singapore;

(k) in relation to a benchmark administrator, means a person (whether a natural, legal person or legal arrangement) –

(i) who provides information to the benchmark administrator in relation to a designated benchmark; or

(ii) with whom the benchmark administrator establishes or intends to establish business relations;

"customer information" means –

(a) in relation to an approved exchange, recognised market operator, approved clearing house and recognised clearing house, "user information" as defined in section 2 of the SFA;

(b) in relation to a licensed trade repository and licensed foreign trade repository, "user information" and "transaction information" as defined in section 2 of the SFA; or

(c) in the case of any other institution, information that relates to its customers and these include customers' accounts, particulars, transaction details and dealings with the financial institutions, but does not include any information that is public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred;

"financial adviser" means a licensed financial adviser under the FAA or a person exempt, under section 23(1)(f) of the FAA read with regulation 27(1)(d) of the FAR, from holding a financial adviser's licence to act as a financial adviser in Singapore in respect of any financial advisory service;

"institution" means any financial institution as defined in section 27A of the Monetary Authority of Singapore Act (Cap. 186);

"material outsourcing arrangement" means 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;

"legal arrangement" means a trust or other similar arrangement;

"legal person" means an entity other than a natural person that can establish a permanent customer relationship with a financial institution or otherwise own property;

"outsourcing agreement" means a written agreement setting out the contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in an outsourcing arrangement;

"outsourcing arrangement" means an arrangement in which a service provider provides the institution with a service that may currently or potentially be performed by the institution itself and which includes the following characteristics –

(a) the institution is dependent on the service on an ongoing basis; and

(b) the service is integral to the provision of a financial service by the institution or the service is provided to the market by the service provider in the name of the institution;

"relevant business transaction" –

(a) in relation to a holder of a money-changer's licence means –

(i) a money-changing transaction of an aggregate value not less than S$5,000; or

(ii) an inward remittance transaction from another country or jurisdiction to Singapore; or

(b) in relation to a holder of a remittance license means, a remittance transaction whether from Singapore to another country or jurisdiction or from another country or jurisdiction to Singapore;

"service provider" means any party which provides a service to the institution, including any entity within the institution's group[4], whether it is located in Singapore or elsewhere;

"sub-contracting" means an arrangement where a service provider which has an outsourcing arrangement with an institution, further outsources the services or part of the services covered under the outsourcing arrangement to another service provider.

4 ENGAGEMENT WITH MAS ON OUTSOURCING

4.1 Observance of the Guidelines

4.1.1 An institution should be ready to demonstrate to MAS its observance of these Guidelines. This should include submission of its outsourcing register in the template set out in Annex 3 at least annually or upon request.

4.1.2 Where MAS is not satisfied with the institution's observance of the Guidelines, MAS may require the institution to take additional measures to address the deficiencies noted. MAS may also take such non-compliance into account in its assessment of the institution, depending on the potential impact of the outsourcing on the institution and the financial system, severity of the deficiencies noted, the institution's track record in internal controls and risk management, and also on the circumstances of the case. MAS may directly communicate with the home or host regulators of the institution and the institution's service provider, on their ability and willingness to cooperate with MAS in supervising the outsourcing risks to the institution.

4.1.3 MAS may require an institution to modify, make alternative arrangements or re-integrate an outsourced service into the institution where one of the following circumstances arises:

(a) An institution fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the outsourcing arrangement;

[4] This refers to the institution's Head Office or parent institution, subsidiaries, affiliates, and any entity (including their subsidiaries, affiliates and special purpose entities) that the institution exerts control over or that exerts control over the institution.

(b) An institution fails or is unable to implement adequate measures to address the risks arising from its outsourcing arrangements in a satisfactory and timely manner;

(c) Adverse developments arise from the outsourcing arrangement that could impact an institution;

(d) MAS' supervisory powers over the institution and ability to carry out MAS' supervisory functions in respect of the institution's services are hindered; or

(e) The security and confidentiality of the institution's customer information is lowered due to changes in the control environment of the service provider.

4.2 Notification of Adverse Developments

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

5 RISK MANAGEMENT PRACTICES

5.1 Overview

5.1.1 In supervising an institution, MAS will review its implementation of these Guidelines, the quality of its board and senior management oversight and governance, internal controls and risk management with regard to managing outsourcing risks.

5.2 Responsibility of the Board and Senior Management

5.2.1 The board and senior management of an institution play pivotal roles in ensuring a sound risk management culture and environment. While an institution may delegate day-to-day operational duties to the service provider, the responsibilities for maintaining effective oversight and governance of outsourcing arrangements, managing outsourcing risks, and implementing an adequate outsourcing risk management framework, in accordance with these Guidelines, continue to rest with the institution, its board and senior management. The board and senior management of an institution should ensure there are adequate processes to provide a comprehensive institution-wide view of the institution's risk exposures from outsourcing, and incorporate the assessment and mitigation of such risks into the institution's outsourcing risk management framework.

5.2.2 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 policies that apply to such arrangements;

(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, such as a management body that reviews controls for consistency and alignment with a comprehensive institution-wide view of risk; and

(f) undertaking regular reviews of these outsourcing strategies and arrangements for their continued relevance, and safety and soundness.

5.2.3 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 institution'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.

5.2.4 Where the board delegates its responsibility to a committee as described in paragraph 5.2.2, the board should establish communication procedures between the board and the committee. This should include requiring the committee to report to the board on a regular basis, and ensuring that senior management is held responsible for implementation of the guidelines as elaborated in paragraphs 5.2.3 (a) to 5.2.3 (h). Notwithstanding the delegation of responsibility to a committee, the board shall remain responsible for the performance of its responsibilities by that committee.

5.2.5 For an institution incorporated or established outside Singapore, the functions of the board described in paragraph 5.2.2 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 (e.g., a regional risk management committee). The functions of senior management in paragraph 5.2.3 lie with local management. Local management of an institution incorporated or established outside Singapore should continue to take necessary steps to enable it to discharge its obligations to comply with the relevant laws and regulations in Singapore, including expectations under these Guidelines. Local management cannot abrogate its governance responsibilities to run the institution in a prudent and professional manner.

5.3 Evaluation of Risks

5.3.1 In order to be satisfied that an outsourcing arrangement does not result in the risk management, internal control, business conduct or reputation of an institution being compromised or weakened, the board and senior management would need to be fully aware of and understand the risks arising from outsourcing. The institution should establish a framework for risk evaluation which should include the following steps:

(a) identifying the role of outsourcing in the overall business strategy and objectives of the institution;

(b) performing comprehensive due diligence on the nature, scope and complexity of the outsourcing arrangement to identify and mitigate key risks;

(c) assessing[5] the service provider's ability to employ a high standard of care in performing the outsourced service and meet regulatory standards as expected of the institution, as if the outsourcing arrangement is performed by the institution;

(d) analysing the impact of the outsourcing arrangement on the overall risk profile of the institution, and whether there are adequate internal expertise and resources to mitigate the risks identified;

(e) analysing the institution's as well as the institution's group aggregate exposure to the outsourcing arrangement, to manage concentration risk; and

(f) analysing 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, and unexpected termination in the outsourcing arrangement, and whether for strategic and internal control reasons, the institution should not enter into the outsourcing arrangement.

5.3.2 Such risk evaluations should be performed when an institution 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, as part of the approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the institution.

5.4 Assessment of Service Providers

5.4.1 In considering, renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.

5.4.2 An institution should assess all relevant aspects of the service provider, including its capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the institution to meet its obligations as a regulated entity. The due diligence should also take into account the physical and IT security

[5] Please see paragraph 5.4 on assessment of service providers.

controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement. Onsite visits to the service provider, and where possible, independent reviews and market feedback on the service provider, should also be obtained to supplement the institution's assessment. Onsite visits should be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.

5.4.3 The due diligence should involve an evaluation of all relevant information about the service provider. Information to be evaluated includes the service provider's:

(a) experience and capability to implement and support the outsourcing arrangement over the contracted period;

(b) financial strength and resources (the due diligence should be similar to a credit assessment of the viability of the service provider based on reviews of business strategy and goals, audited financial statements, the strength of commitment of major equity sponsors and ability to service commitments even under adverse conditions);

(c) corporate governance, business reputation and culture, compliance, and pending or potential litigation;

(d) security and internal controls, audit coverage, reporting and monitoring environment;

(e) risk management framework and capabilities, including technology risk management[6] and business continuity management[7] in respect of the outsourcing arrangement;

(f) disaster recovery arrangements and disaster recovery track record;

(g) reliance on and success in dealing with sub-contractors;

(h) insurance coverage;

(i) external environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates); and

[6] Standards should be commensurate with that expected of the institution as set out in MAS' Technology Risk Management Guidelines.

[7] Standards should be commensurate with that expected of the institution as set out in MAS' Business Continuity Management Guidelines. Please also see paragraph 5.7 of the Guidelines on Outsourcing for more guidance.

(j) ability to comply with applicable laws and regulations and track record in relation to its compliance with applicable laws and regulations.

5.4.4 The institution should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the institution's hiring policies for the role they are performing, consistent with the criteria applicable to its own employees. The following are some non-exhaustive examples of what should be considered under this 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.

Any adverse findings from this assessment should be considered in light of their relevance and impact to the outsourcing arrangement.

5.4.5 Due diligence undertaken during the assessment process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing arrangements. The due diligence process may vary depending on the nature, and extent of risk of the arrangement and impact to the institution in the event of a disruption to service or breach of security and confidentiality (e.g., reduced due diligence may be sufficient where the outsourcing arrangements are made within the institution's group[8]). An institution should ensure that the information used for due diligence evaluation is sufficiently current. An institution should also consider the findings from the due diligence evaluation to determine the frequency and scope of audit on the service provider.

5.5 Outsourcing Agreement

5.5.1 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

[8] Please see paragraph 5.11 on arrangements relating to outsourcing within a group.

also be vetted by a competent authority (e.g., the institutions' legal counsel) on their legality and enforceability.

5.5.2 An institution 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 at the very least, 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[9];

(d) business continuity management[10];

(e) monitoring and control[11];

(f) audit and inspection[12];

(g) Notification of adverse developments
An institution should specify in its outsourcing agreement the type of events and the circumstances under which the service provider should report to the institution in order for an institution to take prompt risk mitigation measures and notify MAS of such developments under paragraph 4.2.1;

(h) Dispute resolution
An institution should specify in its outsourcing agreement the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties in the agreement. The institution should ensure that its contractual rights can be exercised in the event of a breach of the outsourcing agreement by the service provider;

(i) Default termination and early exit
An institution should, have the right to terminate the outsourcing agreement in the event of default, or under circumstances where:
(i) the service provider undergoes a change in ownership;

[9] Refer to paragraph 5.6

[10] Refer to paragraph 5.7

[11] Refer to paragraph 5.8

[12] Refer to paragraph 5.9

(ii) the service provider becomes insolvent or goes into liquidation;
(iii) the service provider goes into receivership or judicial management whether in Singapore or elsewhere;
(iv) there has been a breach of security or confidentiality; or
(v) there is a demonstrable deterioration in the ability of the service provider to perform the contracted service.

The minimum period to execute a termination provision should be specified in the outsourcing agreement. Other provisions should also be put in place to ensure a smooth transition when the agreement is terminated or being amended. Such provisions may facilitate transferability of the outsourced services to a bridge-institution or a third party. Where the outsourcing agreement involves an intra-group entity, the agreement should be legally enforceable against the intra-group entity providing the outsourced service;

(j) Sub-contracting

An institution should retain the ability to monitor and control its outsourcing arrangements when a service provider uses a sub-contractor. An outsourcing agreement should contain clauses setting out the rules and limitations on sub-contracting. An institution should include clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractor and for the sub-contractor's compliance with the provisions in its agreement with the service provider, including the prudent practices set out in these Guidelines. The institution should ensure that the sub-contracting of any part of material outsourcing arrangements is subject to the institution's prior approval;

(k) Applicable Laws

Agreements should include choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.

5.5.3 Each agreement should be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside Singapore[13].

[13] Refer to paragraph 5.10.

5.6 Confidentiality and Security

5.6.1 As public confidence in institutions is a cornerstone in the stability and reputation of the financial industry, it is vital that an institution satisfies itself that the service provider's security policies, procedures and controls will enable the institution to protect the confidentiality and security of customer information.

5.6.2 An institution should be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. An institution should take the following 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, including the circumstances under which each party has the right to change security requirements. The outsourcing agreement should also address:

(i) the issue of the party liable for losses in the event of a breach of security or confidentiality and the service provider's obligation to inform the institution; and

(ii) the issue of access to and disclosure of customer information by the service provider. Customer information should be used by the service provider and its staff strictly for the purpose of the contracted service;

(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, particularly where multi-tenancy[14] arrangements are present at the service provider; and

(d) Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose to the institution breaches of confidentiality in relation to customer information.

[14] Multi-tenancy generally refers to a mode of operation adopted by service providers where a single computing infrastructure (e.g., servers, databases etc.) is used to serve multiple customers (tenants).

5.7 Business Continuity Management

5.7.1 An institution should ensure that its business continuity is not compromised by outsourcing arrangements, in particular, of the operation of its critical systems as stipulated under the Technology Risk Management Notice. An institution should adopt the sound practices and standards contained in the Business Continuity Management ("BCM") Guidelines issued by MAS, in evaluating the impact of outsourcing on its risk profile and for effective BCM.

5.7.2 In line with the BCM Guidelines, an institution should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated such that the institution remains 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. Such tests would serve to familiarise the institution and the service provider with the recovery processes as well as improve the coordination between the parties involved. The institution should require the service provider to notify it of any test finding that may affect the service provider's performance. The institution should also require the service provider to notify it of any substantial changes in the service provider's BCP plans and of any adverse development that could substantially impact the service provided to the institution; 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.

5.7.3 For assurance on the functionality and effectiveness of its BCP plan, an institution should design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement. For tests to be complete and meaningful, the institution should involve the service provider in the validation of its BCP and assessment of the awareness and preparedness of its own staff. Similarly, the institution should take part in its service providers' BCP and disaster recovery exercises.

5.7.4 The institution should consider worst case scenarios in its business continuity plans. Some examples of these scenarios are unavailability of service provider due to unexpected termination of the outsourcing agreement, liquidation of the service provider and wide-area disruptions that result in collateral impact on both the institution and the service provider. Where the interdependency on an institution in the financial system is high[15], the institution should maintain a higher state of business continuity preparedness. The identification of viable alternatives for resuming operations without incurring prohibitive costs is also essential to mitigate interdependency risk.

5.8 Monitoring and Control of Outsourcing Arrangements

5.8.1 An institution should establish a structure for the management and control of its outsourcing arrangements. Such a structure will vary depending on the nature and extent of risks in the outsourcing arrangements. As relationships and interdependencies in respect of outsourcing arrangements increase in materiality and complexity, a more rigorous risk management approach should be adopted. An institution also has to be more proactive in its relationship with the service provider (e.g., having frequent meetings) to ensure that performance, operational, internal control and risk management standards are upheld. An institution should ensure that outsourcing agreements with service providers contain clauses to address the institution's monitoring and control of outsourcing arrangements.

5.8.2 An institution should put in place all the following measures for effective monitoring and control of any material outsourcing arrangement:

(a) Maintain a register of all material outsourcing arrangements and ensure that the register is readily accessible for review by the board and senior

[15] In MAS' BCM Guidelines, these institutions are referred to as Significantly Important Institutions.

management of the institution. Information maintained in the register should include those set out in Annex 3. The register should be updated promptly and form part of the oversight and governance reviews undertaken by the board and senior management of the institution, similar to those described in paragraph 5.2;

(b) 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. The institution should allocate sufficient resources, in terms of both time and skilled manpower, to the management groups to enable its staff to adequately plan and oversee the entire outsourcing lifecycle;

(c) Establish outsourcing management control groups to monitor and control the outsourced service on an ongoing basis. There should be policies and procedures to monitor service delivery and the confidentiality and security of customer information, for the purpose of gauging ongoing compliance with agreed service levels and the viability of the institution's operations. Such monitoring should be regular and validated through the review of reports by auditors of the service provider or audits commissioned by the institution;

(d) Periodic reviews, at least on an annual basis, on all material outsourcing arrangements. This is to ensure that the institution's outsourcing risk management policies and procedures, and these Guidelines, are effectively implemented. Such reviews should ascertain the adequacy of internal risk management and management information systems established by the institution (e.g., assessing the effectiveness of processes and metrics used to evaluate the performance and security of the service provider) and highlight any deficiency in the institution's systems of control;

(e) <u>Reporting policies and procedures</u>
Reports on the monitoring and control activities of the institution should be reviewed by its senior management [16] and provided to the board for information. The institution should ensure that monitoring metrics and performance data are not aggregated with those belonging to other customers of the service provider. The institution should also ensure that any adverse development arising in any outsourcing arrangement is brought

[16] Refer to paragraph 5.2.3.

to the attention of the senior management of the institution and service provider, or to the institution's board, where warranted, on a timely basis. When adverse development occurs, prompt actions should be taken by an institution to review the outsourcing relationship for modification or termination of the agreement; and

(f) 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.

5.9 Audit and Inspection

5.9.1 An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives.

5.9.2 An institution should include, in all its outsourcing agreements for material outsourcing arrangements, clauses 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 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 institution to:

(i) access and inspect the service provider and its sub-contractors, and 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

(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, in relation to the outsourcing arrangement.

5.9.3 Outsourcing agreements for material outsourcing arrangements should also include clauses that require the service provider to comply, as soon as possible, with any request from MAS or the institution, 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.

5.9.4 An institution should 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 institution reasonable notice of its intent to exercise its inspection rights and share its findings with the institution where appropriate.

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 scope of the audits and expert assessments should include an assessment of the service providers' and its sub-contractors' security[17] and control environment, incident management process (for material breaches, service disruptions or other material issues) and the institution's observance of these Guidelines in relation to the outsourcing arrangement.

5.9.6 The independent audit and/or expert assessment on the service provider and its sub-contractors may be performed by the institution's internal or external auditors, the service provider's external auditors[18] or by agents appointed by the institution. 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[19]. Institutions 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 institution 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.

[17] The security environment refers to both the physical and IT security environments.

[18] An institution should conduct its own audits to supplement the audits performed by the service provider's auditors, where necessary.

[19] Please refer to para 5.2 on Responsibilities of Board and Senior Management

5.9.7 Significant issues and concerns should be brought to the attention of the senior management of the institution and service provider, or to the institution's board, where warranted, on a timely basis. Actions should be taken by the institution to review the outsourcing arrangement if the risk posed is no longer within the institution's risk tolerance.

5.9.8 Copies of audit reports should be submitted by the institution to MAS. An institution should also, upon request, provide MAS with other reports or information on the institution and service provider that is related to the outsourcing arrangement.

5.10 Outsourcing Outside Singapore

5.10.1 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 an institution to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the institution. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the institution. In its risk management of such outsourcing arrangements, an institution should take into account, as part of its due diligence, and on a continuous basis:

(a) government policies;

(b) political, social, economic conditions;

(c) legal and regulatory developments in the foreign country; and

(d) the institution's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.

The institution should also be aware of the disaster recovery arrangements and locations established by the service provider in relation to the outsourcing arrangement. As information and data could be moved to primary or backup sites located in foreign countries, the risks associated with the medium of transport, be it physical or electronic, should also be considered.

5.10.2 Material outsourcing arrangements with service providers located outside Singapore should be conducted in a manner so as not to hinder MAS' efforts to supervise the Singapore business activities of the institution (i.e., from its books, accounts and documents) in a timely manner, in particular:

(a) An institution should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements.

(b) An institution 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. An institution must at least commit to retrieve information readily from the service provider should MAS request for such information. The institution should confirm in writing to MAS, that the institution 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, as set out in paragraph 5.9.

(c) An institution should notify MAS if any overseas authority were to seek access to its customer information or if a situation were to arise where the rights of access of the institution and MAS set out in paragraph 5.9, have been restricted or denied.

5.11 Outsourcing Within a Group

5.11.1 These Guidelines are applicable to outsourcing arrangements with parties within an institution's group. The expectations may be addressed within group-wide risk management policies and procedures. The institution would be 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. For an institution incorporated or established outside Singapore, the roles and responsibilities of the local management are set out in paragraph 5.2.5.

5.11.2 Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects of the service provider's ability to address risks specific to the institution, particularly those relating to business continuity management, monitoring and control, audit and inspection, including 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 should be documented in writing in a service level agreement or an equivalent document.

5.12 Outsourcing of Internal Audit to External Auditors

5.12.1 Where the outsourced service is the internal audit function of an institution, there are additional issues that an institution should deliberate upon. One of these is the lack of

independence or the appearance of impaired independence, when a service provider is handling multiple engagements for an institution, such as internal and external audits, and consulting work. There is doubt that the service provider, in its internal audit role, would criticise itself for the quality of the external audit or consultancy services provided to the institution. In addition, as operations of an institution could be complex and involve large transaction volumes and amounts, it should ensure service providers have the expertise to adequately complete the engagement. An institution should address these and other relevant issues before outsourcing the internal audit function. In addition, as a sound practice, institutions should not outsource their internal audit function to the institution's external audit firm[20].

5.12.2 Before outsourcing the internal audit function to external auditors, an institution should satisfy itself that the external auditor would be in compliance with the relevant auditor independence standards of the Singapore accounting profession.

6 CLOUD COMPUTING

6.1 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 typically delivered in the form of Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

6.2 CS can potentially offer a number of advantages, which include economies of scale, cost-savings, access to quality system administration well as operations that adhere to uniform security standards and best practices. CS may also be used to provide the flexibility and agility for institutions to scale up or pare down on computing resources quickly as usage requirements change, without major hardware and software outlay as well as lead-time. In addition, the distributed nature of CS may enhance system resilience during location-specific disasters or disruptions.

6.3 It has been noted that more and more institutions are adopting CS to fulfil their business and operational requirements. These CS deployments may be operated in-house or off-premises by service providers. While the latter can take the form of a private[21] or public[22] cloud, there is a growing trend for institutions to adopt a combination of private and public

[20] Any departure from this best practice should be limited to small institutions and should remain within the bounds of the applicable ethical standards for the statutory or external auditor.

[21] A cloud infrastructure operated solely for an organisation

[22] A cloud infrastructure made available to the general public or an industry group, and is owned by a third party service provider

clouds to create a hybrid cloud. The different cloud models provide for distinct operational and security trade-offs.

6.4 In the recent years, cloud technology has evolved and matured considerably and CS providers have become aware of the technology and security requirements of institutions to protect sensitive customer data. In this regard, a number of CS providers have implemented strong authentication, access controls, tokenisation techniques and data encryption to bolster security to meet institutions' requirements.

6.5 MAS considers CS operated by service providers as a form of outsourcing and recognises that institutions may leverage on such a service to enhance their operations and service efficiency while reaping the benefits of CS' scalable, standardised and secured infrastructure.

6.6 The types of risks in CS that confront institutions are not distinct from that of other forms of outsourcing arrangements. Institutions should perform the necessary due diligence and apply sound governance and risk management practices articulated in this set of guidelines when subscribing to CS.

6.7 Institutions should be aware of CS' typical characteristics such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations. Hence, institutions should take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. In particular, institutions should 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.

6.8 Institutions 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 institutions to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the CS.

Annex 1

EXAMPLES OF OUTSOURCING ARRANGEMENTS

1 The following are examples of some services that, when performed by a third party, would be regarded as outsourcing arrangements for the purposes of these Guidelines although they are not exhaustive:

(a) application processing (e.g., loan origination, credit cards);
(b) white-labelling arrangements such as for trading and hedging facilities;
(c) middle and back office operations (e.g., electronic funds transfer, payroll processing, custody operations, quality control, purchasing, maintaining the register of participants of a collective investment scheme (CIS) and sending of accounts and reports to CIS participants, order processing, trade settlement and risk management);
(d) business continuity and disaster recovery functions and activities;
(e) claims administration (e.g., loan negotiations, loan processing, collateral management, collection of bad loans);
(f) document processing (e.g., cheques, credit card and bill payments, bank statements, other corporate payments, customer statement printing);
(g) information systems hosting (e.g., software-as-a-service, platform-as-a-service, infrastructure-as-a-service);
(h) information systems management and maintenance (e.g., data entry and processing, data centres, data centre facilities management, end-user support, local area networks management, help desks, information technology security operations);
(i) investment management (e.g., discretionary portfolio management, cash management);
(j) management of policy issuance and claims operations by managing agents;
(k) manpower management (e.g., benefits and compensation administration, staff appointment, training and development);
(l) marketing and research (e.g., product development, data warehousing and mining, media relations, call centres, telemarketing);
(m) professional services related to the business activities of the institution (e.g., accounting, internal audit, actuarial, compliance);
(n) support services related to archival and storage of data and records; and
(o) calculation of financial benchmarks.

2 The following arrangements would generally not be considered outsourcing arrangements:

(a) Arrangements in which certain industry characteristics require the use of third-party providers

(i) maintenance of custody account with specified custodians as required under Regulation 27 of the Securities and Futures (Licensing and Conduct of Business) Regulations;

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

(iii) postal services;

(iv) market information services (e.g., Bloomberg, Moody's, Standard & Poor's);

(v) common network infrastructure (e.g., Visa, MasterCard, MASNET+);

(vi) clearing and settlement arrangements between clearing houses and settlement institutions and their members, and similar arrangements between members and non-members;

(vii) global financial messaging infrastructure which are subject to oversight by relevant regulators (e.g., SWIFT); and

(viii) correspondent banking services.

(b) Introducer arrangements and arrangements that pertain to principal-agent relationships

(i) sale of insurance policies by agents, and ancillary services relating to those sales;

(ii) acceptance of business by underwriting agents; and

(iii) introducer arrangements (where the institution does not have any contractual relationship with customers).

(c) Arrangements that the institution is not legally or administratively able to provide

(i) statutory audit and independent audit assessments;

(ii) discreet advisory services (e.g., legal opinions, independent appraisals, trustees in bankruptcy, loss adjuster); and

(iii) independent consulting (e.g., consultancy services for areas which the institution does not have the internal expertise to conduct)

Annex 2

MATERIAL OUTSOURCING

1 An institution should assess the materiality in an outsourcing arrangement. In assessing materiality, MAS recognises that qualitative judgment is involved and the circumstances faced by individual institutions may vary. Factors that an institution should consider include:

(a) importance of the business activity to be outsourced (e.g., in terms of contribution to income and profit);

(b) potential impact of the outsourcing on earnings, solvency, liquidity, funding and capital, and risk profile;

(c) impact on the institution's reputation and brand value, and ability to achieve its business objectives, strategy and plans, should the service provider fail to perform the service or encounter a breach of confidentiality or security (e.g., compromise of customer information);

(d) impact on the institution's customers, should the service provider fail to perform the service or encounter a breach of confidentiality or security;

(e) impact on the institution's counterparties and the Singapore financial market, should the service provider fail to perform the service;

(f) cost of the outsourcing as a proportion of total operating costs of the institution;

(g) cost of outsourcing failure, which will require the institution to bring the outsourced activity in-house or seek similar service from another service provider, as a proportion of total operating costs of the institution;

(h) aggregate exposure to a particular service provider in cases where the institution outsources various functions to the same service provider; and

(i) ability to maintain appropriate internal controls and meet regulatory requirements, if the service provider faces operational problems.

2 Outsourcing of all or substantially all of its risk management or internal control functions, including compliance, internal audit, financial accounting and actuarial (other than performing certification activities) is to be considered a material outsourcing arrangement.

3 An institution should undertake periodic reviews of its outsourcing arrangements to identify new outsourcing risks as they arise. An outsourcing arrangement that was previously not material may subsequently become material from incremental services outsourced to the same service provider or an increase in volume or change in nature of the service outsourced to the service provider. Outsourcing risks may also increase when the service provider sub-contracts the service or makes significant changes to its sub-contracting arrangements.

4 An institution should consider materiality at both the institution's level and as a group, i.e., together with the institution's branches and corporations under its control.

Annex 3

REGISTER OF OUTSOURCING ARRANGEMENTS

1 An institution should maintain an updated register of all existing outsourcing arrangements in the format as per the template available from MAS website.