Monetary Authority of Singapore

December 2023

Guidelines on Outsourcing (Banks)

Contents

1. Introduction 3

2. Engagement with MAS 5

3. Risk Management Practices 6

- 3.1 Responsibilities of the Board and Senior Management
- 3.2 Evaluation of risks
- 3.3 Assessment of service providers
- 3.4 Outsourcing agreement
- 3.5 Use of sub-contractor(s)
- 3.6 Confidentiality and Security
- 3.7 Business Continuity Management
- 3.8 Monitoring and control of outsourcing arrangements
- 3.9 Audit and inspection
- 3.10 Outsourcing outside Singapore
- 3.11 Outsourcing within a Group
- 3.12 Outsourcing of Internal Audit to External Auditors

Annex 1 22

Material Outsourcing

Annex 2 23

Cloud Computing

Annex 3 25

Applicablity of Notices and Guidelines for Banks to Different Categories of Services

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 on Outsourcing ("Guidelines") set out the Monetary Authority of Singapore's (MAS) expectations of a bank or merchant bank (hereafter collectively referred to as "Bank") that has entered into or is planning to enter into, an arrangement for ongoing outsourced relevant services ("outsourcing arrangement")[1], with the exception of exempted Outsourced Relevant Services in Annex D of MAS Notices 658 and 1121 ("Notices"). A Bank should conduct a self-assessment of all existing outsourcing arrangements against these Guidelines[2].

1.3. The extent and degree to which a Bank implements the expectations in these Guidelines should be commensurate with the nature of risks in, and materiality of, the outsourcing arrangement, including outsourcing arrangements involving an MAS-regulated entity. A Bank 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 Bank.

1.4. Banks are expected to refer to the Notices in determining which relevant services are outsourcing arrangements. While not the focus of these Guidelines, arrangements outside the definition of an outsourcing arrangement should also be subject to adequate risk management and sound internal controls. Annex 1 provides guidance to a Bank in assessing whether an arrangement would be considered a material outsourcing arrangement. Annex 2 provides guidance on cloud computing. Annex 3 illustrates the requirements and expectations applicable to different types of relevant services for Banks. Please refer to the Notices for the definition of terms used in these Guidelines.

1.5. 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

[1] Includes both material and non-material ongoing outsourcing arrangements.
[2] This includes Banks which are bound by outsourcing arrangements as a result of an acquisition of the business of another institution.

under the relevant legislation, as well as written directions, notices, codes and other guidelines[3] that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation. The Guidelines do not affect and should not be regarded as a statement of the standard of care owed by Banks to their customers.

1.6. These Guidelines take effect on 11 December 2024.

[3] This includes MAS Information Paper on "Operational Risk Management – Third-Party Arrangements", which sets out good practices relating to third-party risk management that MAS expects to see in banks.

2. Engagement with MAS

2.1. A Bank should be able to demonstrate to MAS its observance of the expectations in these Guidelines. Where MAS is not satisfied with the Bank's observance of the expectations in these Guidelines, MAS may require the Bank to take additional measures to address the deficiencies noted, which could include pre-notification of new material ongoing outsourced relevant services (MOORS). MAS may also take non-observance into account in its assessment of the Bank, considering the potential impact of the outsourcing arrangement on the Bank and the financial system, severity of the deficiencies noted, the Bank's track record in internal controls and risk management, and the circumstances of the case. MAS may directly communicate with the home or host regulators of the Bank and the Bank's service provider, on their ability and willingness to cooperate with MAS.

2.2. A Bank should notify MAS as soon as possible of any adverse development arising from its outsourcing arrangements that could impact the Bank. 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 Bank's customer information[4]. A Bank should also notify MAS of such adverse developments encountered within the Bank's group.

[4] Customer information does not include information that is not referable to any customer or named group of customers. This includes information anonymised or encrypted in a secure manner such that the identities of the customers cannot be readily inferred. Customer information which had previously been made public or is otherwise public information would still be considered customer information.

3. Risk Management Practices

3.1 Responsibilities of the Board and Senior Management

3.1.1 The board and senior management of a Bank play pivotal roles in ensuring a sound risk management culture and environment. While a Bank 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 Bank, its board and senior management. The board and senior management of a Bank should ensure there are adequate processes to provide a comprehensive bank-wide view of the Bank's risk exposures from outsourcing, and incorporate the assessment and mitigation of such risks into the Bank's outsourcing risk management framework.

3.1.2 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 Bank 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 bank-wide view of risk; and

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

3.1.3 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 Bank's overall risk profile and risk environment;

(d) monitoring and maintaining effective control of all risks from its MOORS on a bank-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 MOORS to the board in a timely manner.

3.1.4 Where the board delegates its responsibility to a committee as described in paragraph 3.1.2, 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 expectations in these Guidelines as elaborated in paragraph 3.1.3. Notwithstanding the delegation of responsibility to a committee, the board shall remain responsible for the performance of its responsibilities by that committee.

3.1.5 The functions of senior management in paragraph 3.1.3 lie with local management. Local management of a Bank 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 Bank in a prudent and professional manner.

3.2 Evaluation of risks

3.2.1 In order to be satisfied that an outsourcing arrangement does not result in the risk management, internal control, business conduct or reputation of a Bank being compromised or weakened, the board and senior management need to fully appreciate the risks arising from outsourcing. The bank should establish a framework for risk evaluation that includes the following steps:

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

(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 relevant service and meet regulatory standards as expected of the Bank, as if the service is performed by the Bank;

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

(e) analysing the Bank's as well as the Bank'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 of the outsourcing arrangement, and whether for strategic and internal control reasons, the Bank should not enter into the outsourcing arrangement.

3.2.2 Such risk evaluations should be performed when a Bank 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 Bank.

3.2.3 When assessing risks relating to the safeguarding of customer information where the MOORS involves the disclosure of customer information to an overseas service provider, Banks should assess whether it is necessary to obtain independent legal advice or rely on the advice of internal counsel when assessing such risks. The decision on obtaining legal advice and the frequency for obtaining such advice should be approved by the Bank's board, or a committee delegated by it, and whenever there are significant changes in the relevant law(s) overseas.

3.3 Assessment of service providers

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

3.3.2 A Bank 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 Bank to meet its obligations as a regulated entity. The due diligence should also take into account the physical and IT security 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

[5] Please see paragraph 3.3 on assessment of service providers.

service provider, should also be obtained to supplement the Bank's assessment. Onsite visits should be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.

3.3.3 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

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

3.3.4 A Bank should ensure that the employees of the service provider undertaking any part of the outsourcing arrangement have been assessed to meet the Bank'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);

[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 3.7 for more guidance.

(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.

3.3.5 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. A risk-based approach may be used to determine the frequency for the re-performance of due diligence for outsourcing arrangements (including intragroup arrangements). The due diligence process may vary depending on the nature, and extent of risk of the service and impact to the Bank 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 Bank's group[8]). A Bank should ensure that the information used for due diligence evaluation is sufficiently current. A Bank should also consider the findings from the due diligence evaluation to determine the frequency and scope of audit on the service provider.

3.3.6 For the purposes of paragraph 5.2(b) of the Notices on policies on frequencies of checks, a Bank may, but is not required to, set a specific policy for each MOORS. Banks may set policies for groups or types of MOORS so long as banks ensure that the review frequency is commensurate with the risks posed by the MOORS.

3.4 Outsourcing agreement

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

3.4.2 A Bank 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 Bank 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;

[8] Please see paragraph 3.11 on provision of outsourced relevant services within a group.

(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
A Bank should specify in its outsourcing agreement the type of events and the circumstances under which the service provider should report to the Bank in order for the Bank to take prompt risk mitigation measures and notify MAS of such developments under paragraph 2.2;

(h) dispute resolution
A Bank 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 Bank 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[13]

(j) 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.

3.4.3 A Bank should have the right to terminate the outsourcing agreement in the event of default, or under any of the following circumstances:

(a) by giving reasonable notice to the service provider;

(b) if the service provider or a sub-contractor, as the case may be, failed to safeguard the confidentiality or integrity of customer information of the Bank; or

(c) if there has been a demonstrable deterioration in the ability of the service provider or a sub-contractor to safeguard the confidentiality of customer information.

3.4.4 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

[9] The provisions of the outsourcing agreement for a MOORS that relate to confidentiality and security should include the requirements set out in paragraph 7.1(a) to (c) of the Notices. Refer also to paragraph 3.6.
[10] Refer to paragraph 3.7.
[11] Refer to paragraph 3.8.
[12] The provisions of the outsourcing agreement for a MOORS that relate to audit and inspection should include the requirements set out in paragraph 7.1(d) of the Notices. Refer also to paragraph 3.9.
[13] Refer to paragraphs 3.4.3 to 3.4.8.

agreement is terminated or being amended. Such provisions may facilitate transferability of the outsourced services to a bridge-institution[14] 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.

3.4.5 For the purposes of paragraph 7.1(g) in the Notices, MAS will consider directing a Bank to terminate the contract, or to stop obtaining or receiving the MOORS[15], when

(a) circumstances referred to in paragraph 10.3 of the Notices arise and the service provider is unwilling or unable to remediate the issues;
(b) the service provider is unable or unwilling to remediate issues and the Bank did not elect to terminate the outsourcing agreement of its own accord;
(c) a Bank fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the MOORS;
(d) a Bank fails or is unable to implement adequate measures to address the risks arising from its ongoing outsourced relevant services in a satisfactory and timely manner;
(e) adverse developments arise from the MOORS that could impact a Bank;
(f) MAS or an auditor appointed by MAS, is prevented by the service provider from auditing the books, systems and premises of the service provider for any of the purposes mentioned in section 47A(10) of the Banking Act 1970 (the "Act");
(g) where the sub-contracting agreement provides for the matter mentioned in paragraph 3.5.3(b)(iv), the Bank or any auditor appointed by the Bank, is prevented by the sub-contractor from auditing the books, systems and premises of the sub-contractor for any of the purposes mentioned in paragraph 3.5.3(b)(iv); or
(h) where the sub-contracting agreement provides for the matter mentioned in paragraph 3.5.3(b)(v), the Bank, or any person appointed by the Bank, is prevented by the sub-contractor from obtaining any record, document, report or information relating to the sub-contracting arrangement.

3.4.6 MAS will endeavour to provide the Bank reasonable notice of MAS' intent to direct the Bank to terminate its outsourcing arrangement(s).

3.4.7 To better protect its information, a Bank should endeavour for the requirement in paragraph 7.1(f) of the Notices on deleting, destroying or rendering unusable information upon termination to go beyond the minimally required customer information to also include non-customer information given to the service provider, except for situations where the Bank assesses that the service provider has legitimate

[14] "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.

[15] MAS will only direct Banks to terminate outsourcing agreements for MOORS as a last resort. Banks do not have to exercise the termination rights if they are able to work with the service provider to remediate the issues giving rise to the ground(s) for termination.

reason(s) to retain non-customer information. The Bank should also ensure the minimum period to execute a termination provision is specified in the outsourcing agreement.

3.4.8 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[16].

3.5 Use of sub-contractor(s)

3.5.1 A Bank should retain the ability to monitor and control the risks arising from 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. A Bank 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. A Bank should ensure that the sub-contracting of any part of MOORS is subject to the Bank's prior approval.

3.5.2 Before a Bank allows a MOORS that involves the disclosure of customer information to be sub-contracted, it must obtain the written consent of the customer for the Bank to disclose the customer information to the sub-contractor. Such consent need not name the service providers to whom customer information is to be disclosed, though the scope and purpose for the disclosure should be made known[17].

3.5.3 For MOORS, a Bank should take reasonable steps, on a risk proportionate and best effort basis, to ensure that sub-contractors are held to similar standards as service providers. This could be through inclusion of appropriate provisions in its outsourcing agreement with service providers. A Bank should endeavour to ensure the following:

(a) where a sub-contracting arrangement involves the disclosure of customer information to a sub-contractor:

(i) the sub-contractor is notified in writing of the Bank's obligations of confidentiality under the Act and common law;

(ii) customer information is disclosed to, or accessed, collected, copied, modified, used, stored or processed by, a sub-contractor only to the extent that is necessary for the sub-contractor to perform its duties under a sub-contracting arrangement; and

[16] Refer to paragraph 3.10.

[17] For instance, the consent can be obtained via the terms and conditions at the point of onboarding but Banks should take reasonable steps to ensure customers are apprised that they are granting such consent to the Bank.

(iii) the sub-contractor and its employees do not disclose any customer information of the Bank to any third party unless compelled by law, in which case the sub-contractor must notify the Bank directly or through the service provider as soon as practicable to the extent permitted by law;

(b) that a sub-contracting agreement includes the following provisions:

(i) the sub-contractor protects the confidentiality and integrity of all information of the Bank in its custody, in relation to the provision of the MOORS under the sub-contracting arrangement;

(ii) the sub-contractor ensures that it and its employees only access, collect, copy, modify, use, store, or process any customer information of the Bank to the extent that is necessary for it and its employees to provide the MOORS under the sub-contracting arrangement;

(iii) the sub-contractor ensures that it and its employees do not disclose any customer information of the Bank to any third party unless compelled by law, in which case the sub-contractor must notify the Bank directly or through the service provider as soon as practicable to the extent permitted by law;

(iv) MAS, or an auditor appointed by MAS, be allowed to audit the sub-contractor for the purposes of determining whether the sub-contractor is properly providing the MOORS under the sub-contracting arrangement and assessing:

(A) the ability of the sub-contractor to:

(AA) ensure continuity of the MOORS under the sub-contracting arrangement;

(BB) safeguard the confidentiality and integrity of all information in its custody, in relation to the provision of the MOORS under the sub-contracting arrangement; and

(CC) manage its legal, reputational, technological and operational risks arising from the provision of the MOORS under the sub-contracting arrangement; and

(B) the level of compliance of the sub-contractor with written laws related to the provision of the MOORS under the sub-contracting arrangement;

(v) a provision that the sub-contractor, on a request by the Bank, directly or through the service provider, provides to the Bank or MAS, or any person appointed by the Bank or MAS, any record, document, report or information relating to the provision of the MOORS under the sub-contracting arrangement; and

(vi) a provision that if the Bank stops obtaining or receiving the MOORS under the sub-contracting arrangement provided by the sub-contractor, the sub-contractor ensures that customer information[18] given to the sub-contractor are deleted, destroyed or rendered unusable as soon as possible except where:

[18] Banks may provide flexibility to sub-contractors on the deletion of non-customer information.

(A) the sub-contractor is prohibited from doing so by written law or foreign laws, in the case where the MOORS under the sub-contracting arrangement is obtained or received overseas; or

(B) in the case where the sub-contractor is a branch or office, the record, document or information is stored in a system used by the Bank which upon the termination of the sub-contracting agreement, can only be accessed by the Bank.

3.5.4 For the purposes of paragraph 6.3(a) of the Notices, MAS expects the notification[19] to take place no later than 30 days. Where a notification occurs after 30 days, Banks should assess if the service provider has good reasons to do so and work with the service provider to ensure notifications are provided more promptly in the future.

3.6 Confidentiality and Security

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

3.6.2 A Bank should be proactive in identifying and specifying requirements for confidentiality and security for the outsourcing arrangement. A Bank 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 Bank; 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[20] arrangements are present at the service provider; and

[19] This refers to the service provider's notification to the Bank of its engagement of a sub-contractor.

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

(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 Bank breaches of confidentiality in relation to customer information.

3.7 Business Continuity Management

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

3.7.2 In line with the BCM Guidelines, a Bank should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangements can be adequately mitigated such that the Bank remains able to meet its business obligations 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) Incorporate the necessary contractual requirements and verify 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;

(b) Proactively seek assurance on the state of BCP preparedness of the service provider. It should ensure the service provider regularly tests its BCP to ascertain that the recovery objectives can be met. The Bank should require the service provider to notify it of any test finding that may affect the service provider's performance. The Bank should also require the service provider to notify it of any substantial changes in the service provider's BCP and of any adverse development that could substantially impact the service provided to the Bank; and

(c) Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the Bank 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.

3.7.3 A Bank should involve its service providers, where applicable, in the validation and testing of its BCPs to ensure that BCP testing is complete and meaningful, and to gain assurance on the functionality and effectiveness of its BCPs. Similarly, a Bank could take part in its service providers' business continuity

and disaster recovery tests. Such tests would also serve to familiarise the Bank and the service provider with the recovery processes, as well as improve the coordination between the parties involved.

3.7.4 A Bank should consider worst case scenarios in developing its BCPs for its outsourcing arrangements. 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 Bank and the service provider. Where the interdependency on a Bank in the financial system is high, the Bank 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.

3.8 Monitoring and control of outsourcing arrangements

3.8.1 A Bank 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. A Bank 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. A Bank should ensure that outsourcing agreements with service providers contain clauses to address the Bank's monitoring and control of outsourcing arrangements.

3.8.2 A Bank should put in place all the following measures for effective monitoring and control of any MOORS:

(a) Maintain a register[21] of outsourcing arrangements and ensure that the register is readily accessible for review by the board and senior management of the Bank. The register should be updated promptly and form part of the oversight and governance reviews undertaken by the board and senior management of the Bank, similar to those described in paragraph 3.1;

(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 Bank 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 relevant 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 Bank's operations. Such

[21] Banks should submit their registers according to the template set out at this *link*.

monitoring should be regular and validated through the review of reports by auditors of the service provider or audits commissioned by the Bank;

(d) Reporting policies and procedures
Reports on the monitoring and control activities of the Bank should be reviewed by its senior management[22] and provided to the board for information. The Bank should ensure that monitoring metrics and performance data are not aggregated with those belonging to other customers of the service provider. The Bank should also ensure that any adverse development arising in any outsourcing arrangement is brought to the attention of the senior management of the Bank and service provider, or to the Bank's board, where warranted, on a timely basis. When an adverse development occurs, prompt actions should be taken by a Bank to review the outsourcing relationship for modification or termination of the agreement; and

(e) 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.

3.9 Audit and inspection

3.9.1 A Bank's outsourcing arrangements should not interfere with the ability of the Bank to effectively manage its business activities or impede MAS in carrying out its supervisory functions.

3.9.2 A Bank should include, in all its outsourcing agreements for MOORS, clauses that allow the Bank to conduct audits on the service provider and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the Bank. The Bank should also 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.

3.9.3 A Bank should endeavour to subject any sub-contractor, that a service provider (including any disaster recovery and backup service providers) may engage in the Bank's MOORS, to the audit requirements and expectations applied to the service provider. MAS will endeavour to provide the Bank reasonable notice of MAS' intent to exercise its inspection rights and share its findings with the Bank where appropriate.

3.9.4 A Bank should ensure that independent audits and/or expert assessments of its outsourcing arrangements are conducted. In determining the frequency of audit and expert assessment, the Bank should consider the nature and extent of risk and impact to the Bank from the outsourcing

[22] Refer to paragraph 3.1.3.

arrangements. The scope of the audits and expert assessments should include an assessment of the service providers' and its sub-contractors' security[23] and control environment, incident management process (for material breaches, service disruptions or other material issues) and the Bank's observance of the expectations in these Guidelines in relation to the outsourcing arrangement.

3.9.5 The independent audit and/or expert assessment on the service provider and its sub-contractors may be performed by the Bank's internal or external auditors, the service provider's external auditors[24] or by agents appointed by the Bank (e.g. audits commissioned by multiple Banks using the same service provider). The appointed persons should possess the requisite knowledge and skills to perform the audit, 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[25]. Banks and 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 Bank 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.

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

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

3.9.8 Audits and/or expert assessments performed as part of a certification process (but not self-attestations) may be relied on to meet requirements or expectations on audit provided that such audit or assessments are performed by independent and competent auditors. A Bank must also satisfy itself that the audit's scope and methodology allow the Bank to determine the ability of the service provider to perform the outsourcing arrangement (e.g. design, implementation and effectiveness of controls) and the adequacy of the service provider's risk management framework and capabilities. Audit reports must fulfil requirements set out in the Notices. Banks may also rely on pooled audits or third-party certification (of their service providers) performed by independent parties.

[23] The security environment refers to both the physical and IT security environments.
[24] While audits need not be procured by banks, a bank should conduct its own audits to supplement the audits performed by the service provider's auditors, where necessary.
[25] Please refer to paragraph 3.1 on Responsibilities of Board and Senior Management.

3.10 Outsourcing outside Singapore

3.10.1 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 a Bank to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the Bank. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the Bank. In its risk management of such outsourcing arrangements, a Bank 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 Bank's ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy.

A Bank 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.

3.10.2 MOORS 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 Bank (i.e. from its books, accounts and documents) in a timely manner, in particular:

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

(b) A Bank 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. A Bank must at least commit to retrieve information readily from the service provider should MAS request for such information.

3.11 Outsourcing within a Group

3.11.1 These Guidelines are applicable to outsourcing arrangements with parties within a Bank's group, including subsidiaries of Singapore-incorporated banks. The expectations may be addressed within group-wide risk management policies and procedure. The Bank 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 a Bank incorporated or established outside Singapore, the roles and responsibilities of the local management are set out in paragraph 3.1.5.

3.11.2 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 Bank, 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 Bank, 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.

3.12 Outsourcing of Internal Audit to External Auditors

3.12.1 Where the outsourced service is the internal audit function of a Bank, there are additional issues that a Bank 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 a Bank, 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 Bank. In addition, as operations of a Bank could be complex and involve large transaction volumes and amounts, it should ensure service providers have the expertise to adequately complete the engagement. A Bank should address these and other relevant issues before outsourcing the internal audit function. In addition, as a sound practice, a Bank should not outsource its internal audit function to the Bank's external audit firm[26].

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

3.12.3 A Bank should conduct periodic assessments to satisfy itself of the continuing ability of the service provider to perform the internal audit function satisfactorily. These may include assessments that are in line with the Quality Assurance and Improvement Program as per the International Standards for the Professional Practice of Internal Auditing.

[26] Any departure from this best practice should remain within the bounds of the applicable ethical standards for the statutory or external auditor.

Annex 1

Material Outsourcing

1. A Bank should assess the materiality in an outsourcing arrangement. In assessing materiality, MAS recognises that qualitative judgment is involved and the circumstances faced by Banks may vary. Factors that a Bank 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 Bank'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 Bank's customers, should the service provider fail to perform the service or encounter a breach of confidentiality or security;
   (e) impact on the Bank'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 Bank;
   (g) cost of outsourcing failure, which will require the Bank to bring the outsourced activity in-house or seek similar service from another service provider, as a proportion of total operating costs of the Bank;
   (h) aggregate exposure to a particular service provider in cases where the Bank 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. A Bank 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. A Bank should consider materiality at both the Bank's level and as a group, i.e. together with the Bank's branches and corporations under its control.

Annex 2

Cloud Computing

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).

2. CS can potentially offer a number of advantages, which include economies of scale, cost-savings, access to quality system administration as well as operations that adhere to uniform security standards and best practices. CS may also be used to provide the flexibility and agility for Banks 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.

3. It has been noted that more and more Banks 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[27] or public[28] cloud, there is a growing trend for Banks to adopt a combination of private and public clouds to create a hybrid cloud. The different cloud models provide for distinct operational and security trade-offs.

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 Banks 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 Banks' requirements.

5. MAS considers CS operated by service providers as a form of outsourcing and recognises that Banks 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. The types of risks in CS that confront Banks are not distinct from that of other forms of outsourcing arrangements. Banks should perform the necessary due diligence and apply sound governance and risk management practices articulated in this set of Guidelines when subscribing to CS.

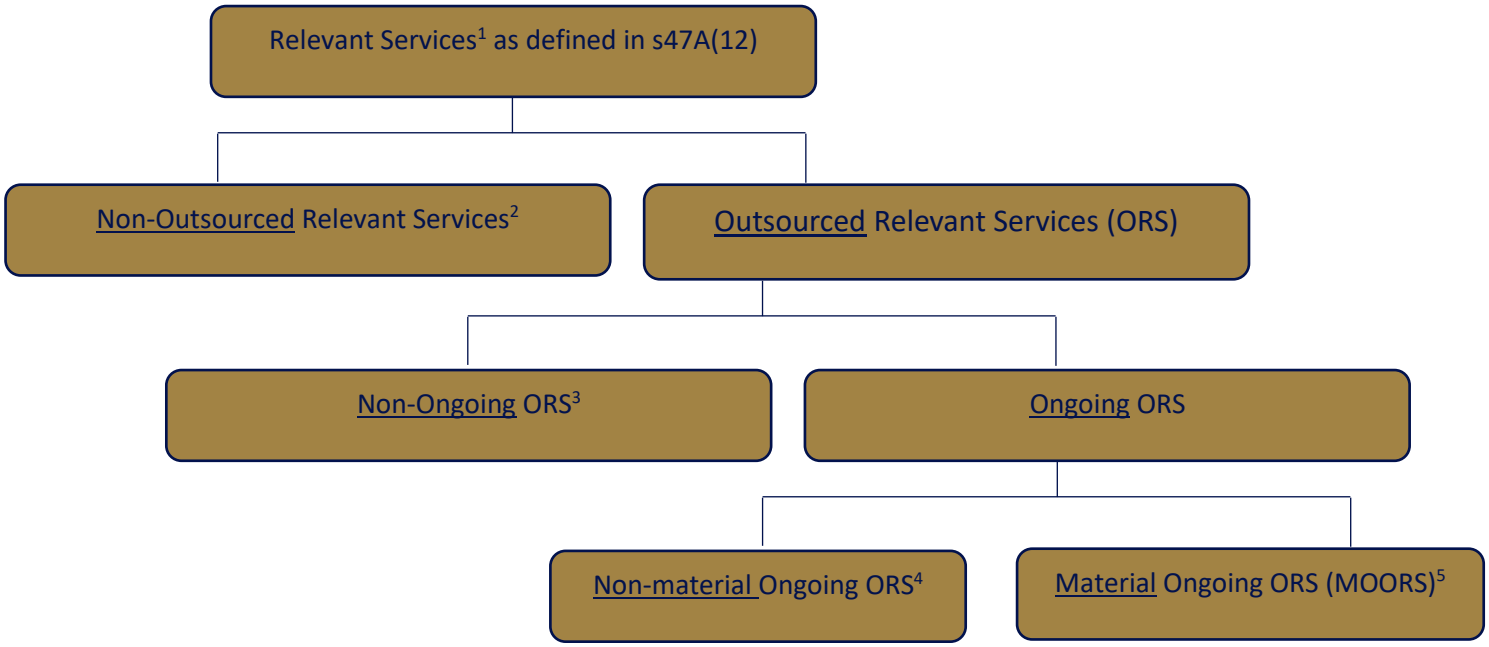
[27] A cloud infrastructure operated solely for an organisation.
[28] A cloud infrastructure made available to the general public or an industry group, and is owned by a third-party service provider.

7. Banks 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, Banks should take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. In particular, Banks 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.

8. Banks 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 Banks to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the CS.

Annex 3

Applicablity of Notices and Guidelines for Banks to Different Categories of Services



1: A "relevant service" means any service obtained or received by the bank, other than a service provided in the course of employment by an employee of the bank or a service provided by a director or an officer of the bank in the course of the director's or officer's appointment, and does not include any service specified by the Authority by written notice.

2: Not subject to Notices and Guidelines for Banks. Non-ORS should still be subject to adequate risk management and sound internal controls.

3: Not subject to Notices and Guidelines for Banks except where ORS involves disclosure of customer information and if so, Section C of Notices and the requirement on outsourcing register in Notices apply. Non-ongoing ORS should still be subject to adequate risk management and sound internal controls.

4: Subject to requirement on outsourcing register in Notices, as well as Section C of Notices where ORS involves disclosure of customer information. Bank should implement expectations in Guidelines to the extent and degree which is commensurate with the nature of risks.

5: Subject to Notices and Guidelines for Banks.