AUTORITI MONETARI BRUNEI DARUSSALAM

Guideline No: ITS/G-1/2015(4)

OUTSOURCING GUIDELINES

1 January 2015

TABLE OF CONTENTS

1 INTRODUCTION

While outsourcing can bring cost and other benefits, it may increase the risk profile of an institution due to, for example, strategic, reputation, compliance and operational risks arising from failure of a service provider in providing the service, breaches in security, or inability to comply with legal and regulatory requirements by the institution. An institution can also be exposed to country risk when a service provider is located overseas and concentration risk when there is a lack of control by a group of institutions over a common service provider. It is therefore important that an institution adopts a sound and responsive risk management framework in outsourcing.

2 APPLICATION OF GUIDELINES

2.1 These Guidelines contain prudent practices on risk management of outsourcing. These 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 these Guidelines should be commensurate with the nature of risks in, and materiality of, the outsourcing. In supervising an institution, AMBD will review its implementation of these Guidelines to assess the quality of risk management systems. AMBD is particularly interested in material outsourcing which, if disrupted, has the potential to significantly impact an institution's business operations, reputation or profitability and which may have systemic implications.

2.2 An institution should notify AMBD when it is planning or has entered into material outsourcing or plan to vary such outsourcing. The institution should expect to engage and demonstrate to AMBD their observance with these Guidelines. AMBD may require additional measures to be taken by an institution and other supervisory actions, depending on the potential impact of the outsourcing on the institution and the financial system. AMBD may also directly communicate with the home and/or host regulator of the institution and its service provider, on their ability and willingness to cooperate with AMBD in supervising the outsourcing risks to the institution.

2.3 A self-assessment should be conducted of all existing outsourcing arrangements against these Guidelines. Where outsourcing is material and has not been notified to AMBD, the institution should do so in writing, within two months from the date of issue of these Guidelines. Every institution is also expected to rectify the deficiencies identified in the self-assessment no later than one year from the date of issue of the Guidelines.

2.4 AMBD should also be notified of any adverse developments arising in outsourcing that could significantly affect the institution, including any events that could potentially lead the termination and early exit of the arrangement. Any breach of legal and regulatory requirements by the service provider should also be notified to AMBD.

2.5 AMBD may require an institution to modify, make alternative arrangements or re-integrate an outsourcing into the institution where :-

- an institution fails or is unable to implement adequate measures to address the risks and deficiencies arising in its outsourcing in a satisfactory and timely manner;
- adverse developments arise from the outsourcing that could significantly affect the institution; or

- AMBD’s supervisory powers and ability to carry out its supervisory functions are hindered.

3 DEFINITIONS

In these Guidelines, unless the context otherwise requires:

‘Board’ or ‘board of directors’ means:

a) In the case of an institution incorporated in Brunei Darussalam, the board of directors.

b) In the case of an institution incorporated or established outside Brunei Darussalam, a management committee or body beyond local management empowered with oversight and supervision responsibilities for the institution in Brunei Darussalam.

‘Institution’ means those companies registered under the Insurance Order, 2006 and the Takaful Order, 2008.

‘Outsourcing’ means an arrangement whereby an institution engages in a third party (the service provider) to provide an institution with a service that may already or may conceivably be performed by the institution itself which includes the following characteristics:

- the institution is dependent on the service on an ongoing basis but excludes services that involve the provision of a finished product;

- the service is integral to the provision of a financial service by the institution and/or the service is provided to the market by the service provider in the name of the institution; and

- it is prohibitive to change the service provider as substitutes are lacking in the market or may only be replaced at significant cost to the institution.

‘Material outsourcing’ means an outsourcing arrangement which, if disrupted, has the potential to significantly impact an institution’s business operations, reputation and profitability.

‘Service provider’ includes a member of the group to which the institution belongs e.g. its Head Office, parent institution, another branch or related company, or an unrelated party, whether located in Brunei Darussalam or elsewhere.

4 LEGAL AND REGULATORY OBLIGATIONS

4.1 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 Brunei Darussalam. Risk management practices should include steps to ensure all relevant laws, regulations, guidelines and other directions, as well as any condition of approval, licensing or registration continue to be met. Supervisory powers over institutions and ability to carry out supervisory functions should also not be hindered, whether the service provider is located within Brunei Darussalam or elsewhere.

4.2 Every institution should conduct its business with integrity and competence. Hence an institution should not engage in outsourcing that results in its internal control, business conduct or reputation being compromised or weakened. An institution has to take steps to ensure that the service provider employs a high standard of care in performing the service as if activity were not outsourced and conducted within the institution. The institution also needs to maintain the capability and appropriate level of monitoring and control over outsourcing, such that in the event of disruption or unexpected termination of the service, it remains able to conduct its business with integrity and competence.

5 MATERIAL OUTSOURCING

An institution should assess the degree of materiality in outsourcing the service to the service provider. In assessing materiality, AMBD recognizes that qualitative judgements involved and the circumstances faced by individual institutions may vary. Factors that an institution should consider include, among others:-

- importance of the business activity to be outsourced, e.g. in terms of contribution to income and profit;
- potential impact of the outsourcing on earnings, solvency, liquidity, funding and capital, and risk profile;
- 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;
- cost of the outsourcing as a proportion of total operating costs of the institution;
- aggregate exposure to a particular service provider in cases where the institution outsources various functions to the same service provider; and
- ability to maintain appropriate internal controls and meet regulatory requirements, if there were operational problems faced by the service provider.

Outsourcing of all or substantially all risk management and internal control functions including compliance, internal audit and financial accounting, is to be considered material.

6 RISK MANAGEMENT PRACTICES

6.1 <u>Role of the Board and Senior Management</u>

6.1.1 The board and the senior management of an institution retain ultimate responsibility for the effective management of risks arising from outsourcing. While an institution may delegate its day-to-day operational duties to the service provider, the responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions, continue to rest with the institution, its board and senior management. The board, or a committee delegated by it, is responsible for:-

- approving framework to evaluate the risks and materiality of all existing and prospective outsourcing and the policies that apply to such arrangements;
- laying down the appropriate authorities for outsourcing depending on the nature of the risks in and materiality of the outsourcing;

- assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures as commensurate with the nature, scope and complexity of the outsourcing arrangements;

- undertaking regular review of outsourcing strategies and arrangements for their continued relevance, and safety and soundness; and

- reviewing a list of all material outsourcing and relevant reports on outsourcing.

6.1.2 Senior management is responsible for:-

- Evaluating the risks and materiality of all existing and prospective outsourcing, based on the framework approved by the board;

- Developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing;

- Reviewing periodically the effectiveness of policies and procedures;

- Communicating information pertaining to material outsourcing risks to the board in a timely manner;

- Ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested; and

- Ensuring that there is independent review and audit for compliance with set policies.

6.2 Evaluation of Risks

6.2.1 To satisfy themselves that an outsourcing does not result in the internal control, business conduct or reputation of an institution being compromised or weakened, its board and senior management would need to be fully aware of and understand the risks in an outsourcing and their impact on the institution. A framework for systematic risk evaluation should be established and it should include the following steps:-

- Identification of the role of outsourcing in the overall business strategy and objectives of the institution and its interaction with corporate strategic goals;

- Comprehensive due diligence on the nature, scope and complexity of the outsourcing to identify the key risks and risk mitigation strategies;

- Analysis of the impact of the arrangement on the overall risk profile of the institution, and whether there are adequate internal expertise and resources to mitigate the risks identified; and

- Analysis of risk-return on the potential benefits of outsourcing against the vulnerabilities that may arise, ranging from the impact of temporary disruption to that of an unexpected termination in the outsourcing, and whether for strategic and internal control reasons, the arrangement should not be entered into.

6.2.2 Such evaluations should be performed when an institution is planning to enter into an outsourcing arrangement, and also re-performed periodically on existing arrangements, as part of the outsourcing approval and strategic planning or review process of the institution.

6.3 Capability of Service Providers

6.3.1 In considering renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due diligence to assess its capability to employ a high standard of care in performing the service and comply with the obligations under the outsourcing agreement. The due diligence should take into consideration qualitative and quantitative, financial, operational and reputation factors. Compatibility and performance should be emphasized in the assessment. The institution should obtain independent reviews and market feedback on the service provider to supplement its own findings.

6.3.2 The due diligence should involve an evaluation of all available information about the service provider such as:-

- its experience and competence to implement and support the proposed activity over the contracted period;

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

- its business reputation and culture, compliance, complaints and outstanding or potential litigation; and

- its business continuity management, insurance coverage and its external factors (such as political, economic, social, legal environment of the jurisdiction in which the service provider operates, and other events) that may impact service performance.

6.3.3 Due diligence undertaken during the selection process should be documented and re-performed periodically as part of the monitoring of control processes of outsourcing. The due diligence process can vary depending on the nature of the outsourcing arrangement e.g. reduced due diligence may be sufficient where no developments or changes have arisen to affect an existing outsourcing arrangement or where the outsourcing is to a member of the group. An institution should ensure that the information used for diligence evaluation is current and should not be more than 12 months old.

6.4 Outsourcing Agreement

6.4.1 Contractual terms and conditions governing relationships, functions, obligations, and responsibilities of the contracting parties in the outsourcing should be carefully and properly defined in written agreements. The detail in these agreements should be appropriate for the nature and materiality of the arrangement. They should also be vetted by a competent authority e.g. the institutions legal counsel on their legal effect and enforceability.

6.4.2 An institution should ensure that every outsourcing agreement addresses the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages. Each agreement should allow for renegotiation and renewal to enable the institution to retain an appropriate level of control over the outsourcing and the right to intervene with the appropriate measures to meet its legal and regulatory obligations. The agreement should also not hinder AMBD in the exercise of its supervisory powers over the institution and right of access to information on the institution and the service provider. It should at the very least, have provisions pertaining to:-

- the scope of the outsourcing service;
- performance standards defined in terms of service levels and performance targets, service, availability, reliability, stability and upgrade;
- confidentiality and security;
- business continuity management;
- monitoring and control;
- audit and inspection;
- dispute resolution;
- default termination and early exit;
- subcontracting;
- applicable laws.

6.5 Confidentiality and Security

6.5.1 An institution should be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. An institution may want to take the following steps to ensure that the issue of customer confidentiality is addressed:-

- Address, agree and document the respective responsibilities of the various parties in the outsourcing 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. It should also address the issue of the party liable for losses in the event of a breach of security and the service provider's obligation to inform the institution.
- Address issues of access and disclosure of customer information provided to the service provider having regard to the institution's obligations under relevant laws and regulations. Customer information should be used by the service provider and its staff strictly for the purpose of the contracted service. Any unauthorized disclosure of the institution's customer information to any party should be prohibited.
- Disclose customer information to the service provider only on a need to know basis and ensure that the amount of information disclosed is commensurate with the requirements of the situation.
- Ensure the service provider is able to isolate and clearly identify the institution's customer information, documents and records and assets to protect the confidentiality of the information. An institution should also ensure that the service provider takes technical, personnel, and organizational measures in order to maintain the confidentiality of customer information between its various customers.

- Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose security breaches.

6.5.2 Confidentiality and security protection should be commensurate with the nature and materiality of the outsourcing. An institution would need to take into consideration any legal or contractual obligation to notify customers of the outsourcing and circumstances under which their information may be disclosed.

6.5.3. An institution should notify AMBD of any unauthorized access or breach of security and confidentiality by the service provider or its sub-contractors that affect the institution or its customers.

6.6 Business Continuity Management (BCM)

6.6.1 An institution should ensure that its business continuity management preparedness is not compromised by outsourcing. It is expected to adopt sound practices and standards, in evaluating the impact of outsourcing on its risk profile and for effective BCM on an ongoing basis.

6.6.2 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 disruption, or unexpected termination of the outsourcing, or liquidation of the service provider. These include steps to:-

- Determine that the service provider has in place satisfactory business continuity plans (BCP) commensurate with the nature, scope and complexity of the outsourcing. Outsourcing agreements should contain BCP requirements on the service provider, in particular recovery time objectives (RTO) and resumption operating capacities. Escalation, activation and crisis management procedures should also be clearly defined.

- Proactively seek assurance on the state of BCP preparedness of the service provider. It should ensure the service provider regularly tests its BCP plans.

- Ensure the service provider is able to isolate and clearly identify the institution's information, documents and records, and other assets such that in adverse conditions, all documents, records of transactions and info given to the service provider, assets of the institution, can be either removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

6.6.3 For assurance on the functionality and effectiveness of its BCP plan, an institution should design and carry out regular complete and meaningful testing of its plans as commensurate with the nature, scope and complexity of the outsourcing, including the risks arising from interdependencies on the institution. For tests to be complete and meaningful, the institution should involve the service provider so as to validate its BCP as well as for assurance on the awareness and preparedness of its own staff. The institution should also base its business continuity considerations and requirements on probable worst case scenarios of unexpected termination of the outsourcing or liquidation of the service provider. Where the interdependency on an institution in the financial system is high, the institution is expected to 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.

6.7 Monitoring and Control of Outsourced Activities

6.7.1 An institution should establish a structure for the management and control of outsourcing. Such a structure will vary depending on the nature, scope and complexity of the outsourced activity. As outsourcing relationships and interdependencies increase in materiality and complexity, a more rigorous risk management approach should be adopted. An institution also has to be more proactive in its relationships with the service provider e.g. having frequent meetings, to ensure that performance levels are upheld. An institution should ensure that outsourcing agreements with service providers contain provisions to address their monitoring and control of outsourced activities.

6.7.2 A structure for effective monitoring and control of material outsourcing would comprise the following:-

- A central record of all material outsourcing that is readily accessible for review by the board and senior management of the institution. Information maintained in the record should include the name and location of the service provider, the value and expiry or renewal dates of the contract, and reviews on the performance of the outsourced arrangement. The record should be updated promptly and form part of the corporate governance reviews undertaken by the board and senior management of the institution

- Multi-disciplinary outsourcing management groups with members from functions including legal, compliance, and finance, to ensure that other than technical issues, legal and regulatory requirements are also met. The institution should allocate sufficient resources to the management group to enable staffs to adequately plan and oversee the entire outsourcing effort.

- Establishment of management control groups to monitor and control the outsourced service on an ongoing basis. There should be policies and procedures to monitor service delivery, performance reliability and processing capacity of the service provider for the purpose of gauging ongoing compliance with agreed service levels and the viability of its operations.

- Regular reviews and audits to ensure outsourcing risk management policies and procedures, and these Guidelines, are being effectively complied with.

- Reporting policies and procedures. Reports on the monitoring and control activities of the institution should be prepared or reviewed by its senior management and provided to its board. The institution should also ensure that any adverse development arising in any outsourced activity is brought to the attention of the senior management of the senior management of the institution and service provider. Actions should be taken by an institution to review the outsourcing relationship for modification or termination of the agreement.

6.7.3 AMBD should be informed if there are any adverse developments or non-compliance with legal and regulatory requirements in an outsourcing arrangement.

6.8 Audit and Inspection

6.8.1 Outsourcing should not interfere with the ability of the institution to effectively manage its activities or impede AMBD in carrying out its supervisory functions and objectives. Every institution is therefore required to take steps to ensure the outsourcing arrangements with the service provider include clauses that allow:-

- The institution to conduct audits on the service provider, 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 in conjunction with the service performed for the institution; and

- AMBD, or any agent appointed by AMBD, to access both the service provider and the institution to obtain records and documents, of transactions, and information of the institution given to, stored at or any processed by the service provider and the right to access any report and finding made on the service provider.

6.8.2 An institution should at least on an annual basis review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider including reports by the service provider's external auditors, should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness by the institution's internal or external auditors, 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 outsourced activity.

6.8.3 In addition to the annual reviews undertaken to assess the capability of service providers as stated, an institution should also periodically commission independent audit and expert assessments on the security and control environment of the service provider. Such assessments and reports on the service provider may be performed and prepared by the institution's internal or external auditors or by agents appointed by the institution.

6.9 Outsourcing Outside Brunei Darussalam

6.9.1 The engagement of a service provider in a foreign country exposes 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, an institution should take into account, at due diligence on a continuous basis, the government policies and political, social, economic and legal conditions in the foreign country and its ability to effectively monitor the service provider and to execute its BCM plans and exit strategy.

6.9.2 Outsourcing outside Brunei Darussalam should be conducted in a manner so as not to hinder efforts to supervise or reconstruct the Brunei activities of the institution. (i.e. from its books, accounts and documents) in a timely manner. Specifically :-

- An institution should, in principle, enter into arrangements only with parties operating in jurisdictions that generally uphold confidentiality clauses and agreements

- It should not outsource to jurisdictions where prompt access to information by AMBD or agents appointed by AMBD 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 AMBD request for such information. The institution should confirm in writing to AMBD, the rights of access to the institution's information, reports and findings at the service provider

- It should notify AMBD if any overseas authority were to seek access to its customer information.

6.9.3 AMBD may require additional measures to be taken by an institution and other supervisory actions, depending on the potential impact of the outsourcing on the institution and the financial system and the financial system, or circumstances warrant. AMBD may also directly communicate with the home or host regulator of the institution and its service provider, on their ability and willingness to cooperate with AMBD in supervising the outsourcing risks to the institution. AMBD may require an institution to terminate or make alternative outsourcing arrangements if the confidentiality of its customer information or the ability of AMBD to carry out its supervisory functions cannot be assured.

6.10 Outsourcing Within a Group

6.10.1 These Guidelines are generally applicable to outsourcing to parties within an institution's group, including its Head Office or parent institution, another branch or related company, whether located within or outside Brunei Darussalam. The requirements may be addressed within group-wide risk management policies and procedures. The institution would be expected to be able 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.

6.10.2 Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects on the ability of the service provider to address risks specific to the institution, particularly those relating to BCM, monitoring and control, and audit and inspection, including confirmation on the right of access to be provided to AMBD 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. AMBD may require additional measures to be taken by an institution and other supervisory actions, depending on the potential impact of the outsourcing on the institution and the financial system, or as circumstances warrant.

6.11 Outsourcing of Internal Audit to External Auditors

6.11.1 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 Brunei accounting profession.