GUIDELINE NO. TIU/G-1/2019/10

GUIDELINES ON OUTSOURCING ARRANGEMENT FOR INSURANCE COMPANIES AND TAKAFUL OPERATORS

1. INTRODUCTION

1.1. These Guidelines are issued pursuant to Section 88 of the Insurance Order, 2006 and section 90 of the Takaful Order, 2008 ("the Orders") to provide guidance on the Notice No. TIU/N-1/2019/11 "Notice on Application for approval of Outsourcing arrangement for Insurance Companies and Takaful operators", and to set standards for sound practices on risk management of material outsourcing arrangements. The extent and degree to which an insurer implements the Guidelines should be commensurate with the nature of risks in, and materiality of, the outsourcing arrangement.

1.2. These Guidelines shall be read in conjunction with the following:

1.2.1. Notice on Corporate Governance for Insurance Companies and Takaful Operators [Notice No. TIU/N-3/2017/7],

1.2.2. Guidelines on Risk Management and Internal Controls for Insurance Companies and Takaful Operators [Guideline No. TIU/G-3/2018/8]; and

1.2.3. any other notices, directives or guidelines, which the Authority may issue from time to time.

1.3. These Guidelines supersede Guideline No. ITS/G-1/2015 (4).

1.4. These Guidelines shall take effect on 1 September 2020.

2. DEFINITIONS

2.1. For the purpose of these Guidelines:

2.1.1. "Board" means the Board of Directors of the company;

2.1.2. "Group" refers to the insurer's Head Office or parent insurer, subsidiaries, affiliates, and any entity (including their subsidiaries, affiliates and special purpose entities) that the insurer exerts control over or that exerts control over the insurer;

2.1.3. “Insurer” means a registered insurance company under Insurance Order, 2006 and a registered takaful operator under Takaful Order, 2008, unless it is otherwise specified;

2.1.4. “Material outsourcing” means an outsourcing arrangement which, if disrupted, has the potential to significantly impact an insurer’s business operations, reputation and profitability;

2.1.5. “Outsourcing” means an arrangement where an insurer engages a third party (the service provider) to provide the insurer with a service that may already or may conceivably be performed by the insurer itself which includes the following characteristics:

a) The insurer is dependent on the service on an ongoing basis but excludes services that involve the provision of a finished product;

b) The service is integral to the provision of a financial service by the insurer and/or the service is provided to the market by the service provider in the name of the insurer; and

c) 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 insurer.

2.1.6. “Service provider” means any party which provides a service to the insurer, including a member of the group to which the insurer belongs, e.g. its Head Office, parent insurer, another branch or related company, whether it is located in Brunei Darussalam or elsewhere.

3. MATERIAL OUTSOURCING

3.1. An insurer should assess the degree of materiality in outsourcing the service to the service provider. In assessing materiality, qualitative judgements may be involved as the circumstances faced by individual insurers may vary. Factors that the insurer should consider include, among others:

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

3.1.2. potential impact of the outsourcing on earnings, solvency, liquidity, funding and capital, and risk profile;

3.1.3. impact on the insurer’s reputation and brand value, and ability to achieve its business objectives, strategy and plans, should the service provider fail to perform the service;

3.1.4. cost of the outsourcing as a proportion of total operating costs of the insurer;

3.1.5. aggregate exposure to a particular service provider in cases where the insurer outsources various functions to the same service provider; and

3.1.6. ability to maintain appropriate internal controls and meet regulatory requirements, if there were operational problems faced by the service provider.

3.2. Activities that are considered to be material for the purpose of these guidelines includes:

3.2.1. all risk management and internal control functions including compliance, internal audit, financial accounting and actuarial (other than performing certification activities);

3.2.2. information systems hosting (e.g. software-as-a-service, platform-as-a-service, infrastructure-as-a-service);

3.2.3. 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); and

3.2.4. business continuity and disaster recovery functions and activities.

4. RISK MANAGEMENT PRACTICES

4.1. Role of the Board and Senior Management

4.1.1. The board and senior management of an insurer retain ultimate responsibility in ensuring a sound risk management culture and environment. While the insurer may delegate its day-to-day operational duties to the service provider, the board and senior management are responsible for maintaining effective due diligence, oversight and management of the outsourcing, accountable for all outsourcing decisions, and implementing an adequate outsourcing risk management framework.

4.1.2. The board and senior management should ensure there are adequate processes to provide a comprehensive view of the insurer's risk exposure from outsourcing, whilst taking into account the assessment and mitigation of such risks into insurer's outsourcing risk management framework.

4.1.3. The board, or a committee (e.g. Risk Management 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 relevant policies;

b) setting an appropriate risk appetite to define the nature and extent of risks that the insurer is willing and capable of assuming from outsourcing;

c) laying down appropriate approval authorities for outsourcing in line with its established strategy and risk appetite;

d) 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;

e) ensuring that senior management establishes appropriate governance structures and processes for sound and prudent risk management (e.g. a management body that reviews controls for consistency and alignment with a comprehensive view of risk);

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

g) reviewing a list of all material outsourcing and relevant reports on outsourcing;

h) ensuring that the outsourcing strategy is consistent with the insurer's overall business strategy, risk appetite and the wider operating environment; and

i) ensuring that the outsourcing framework remains appropriate should there be material changes to size, nature and complexity of the insurer's operations.

4.1.4. Senior management is responsible for:

a) evaluating the risks and materiality of all existing and prospective outsourcing, based on the framework approved by the board or a committee delegated by it;

b) developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing arrangements, as well as ensuring they are implemented effectively;

c) reviewing periodically the effectiveness of, and appropriately adjusting, policies, standards and procedures to reflect changes in the insurer's overall risk profile and risk environment;

d) monitoring and maintaining effective control of all risks from its material outsourcing arrangements on an insurer-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 set policies and procedures;

g) ensuring that appropriate and prompt remedial actions are taken to address audit findings; and

h) communicating information pertaining to material outsourcing risks to the board in a timely manner.

4.1.5. Where the board delegates its responsibility to a board committee as described in paragraph 4.1.3., it should establish communication procedures between itself and the committee. The committee should be required to regularly report to the board, and ensure that senior management is responsible for implementing the guidelines as described in paragraph 4.1.4. Despite the delegation of responsibility to a committee, the board shall remain responsible for the performance of its responsibilities by that committee.

4.1.6. For an insurer incorporated outside Brunei Darussalam, the functions of the board described in 4.1.3. may be delegated to and performed by a management committee or body beyond local management that oversees and supervises the local office (e.g. a regional Risk Management Committee). Depending on the size, scale and nature of the business undertaking, the functions of senior management in paragraph 4.1.4. lie with local management which should continue to take necessary steps to enable it to discharge its obligations to comply with the relevant laws and regulations in Brunei Darussalam, including expectations under these Guidelines. Local management cannot abrogate its governance responsibilities to run the insurer in a prudent and professional manner. Even where these functions does not reside with the local management of the insurer incorporated outside Brunei Darussalam, it should have a thorough understanding of the outsourced activities, including expectations under these Guidelines, in terms of supervisory reporting and other responsibilities that fall under their purview.

4.1.7. In supervising an insurer, AMBD will review the implementation of these Guidelines by the insurer to assess the quality of its board and senior management oversight and governance, internal controls and risk management and the insurer's material outsourcing arrangements.

4.2. Evaluation of Risks

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

a) identification of the role of outsourcing in the overall business strategy and objectives of the insurer together with its interaction with corporate strategic goals;

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

c) assessment of the service provider's ability to employ a high standard of care in carrying out the outsourcing whilst meeting regulatory standards and requirements (as expected of the insurer), as if the outsourcing was performed by the insurer;

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

e) analysis of the insurer's and its group aggregate exposure to the outsourcing arrangement, to manage concentration risk; and

f) 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 outsourcing arrangement should not be entered into.

4.2.2. Such risk evaluations should be performed when an insurer is planning to enter into an outsourcing arrangement with an existing or a new service provider, and also re-performed periodically on existing arrangements, as part of the outsourcing approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the insurer.

4.3. Assessment of Service Providers

4.3.1. Comprehensive and rigorous assessments on potential service providers are critical and should be conducted. Equally, it is important to periodically evaluate the performance of the service provider against the performance measures as agreed in the outsourcing agreement. This is to ensure that the service is performed to the level expected and that the arrangement remains consistent with the insurer.

4.3.2. Before entering into an outsourcing arrangement and when considering whether to renegotiate or renew an outsourcing arrangement, an insurer should also subject the service provider to appropriate due diligence to assess the risks associated with the outsourcing arrangements.

4.3.3. The insurer should assess all relevant aspects of the service provider. This includes its capability to employ a high standard of care in performing the service, as if it is performed by the insurer to meet its obligations as a regulated entity, and, comply with the obligations under the outsourcing agreement. The due diligence should consider the physical and IT security controls, business reputation and financial strength of the service provider, including the ethical and professional standards held by it, and its ability to meet obligations under the arrangement qualitative and quantitative, financial, operational and reputation factors. Compatibility and performance should be emphasised in the assessment. The insurer should use its findings from onsite visits, independent reviews and market feedback on the service provider to supplement its assessment.

4.3.4. The due diligence should involve an evaluation of all relevant information about the service provider and cover:

a) its experience and competence to implement and support the proposed activity over the contracted period at a high standard;

b) 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);

c) corporate governance, business reputation and culture, compliance, complaints and outstanding or potential litigation;

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

e) risk management framework and capabilities, including technology risk management and business continuity management (with regard to the outsourcing arrangement);

f) disaster recovery arrangements, locations (primary and backup sites) and track record;

g) reliance on and degree of control over the sub-contractors, if any;

h) insurance coverage;

i) 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;

j) ability to comply with applicable laws and regulations, and its track record in relation to this; and.

k) any potential conflict of interest, taking into account the service provider's fee structure and incentives for similar business arrangement with the insurer.

4.3.5. The insurer should ensure that key persons of the service provider who undertake any part of the outsourcing meet the insurer's expectation for the role concerned, which may be consistent with the criteria applicable to its own employees. Any adverse findings from this assessment should be considered in light of their relevance and impact to the outsourcing arrangement.

4.3.6. Due diligence undertaken during the selection process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing arrangements. The due diligence process can vary depending on the nature, and extent of risk of the 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 within the insurer's group). The insurer should ensure that the information used for diligence evaluation is current and should not be more than 12 months old. The insurer should also consider the findings from the due diligence evaluation, and use them to determine the frequency and scope of audit on the service provider.

4.4. <u>Outsourcing Agreement</u>

4.4.1. Contractual terms and conditions governing relationships, functions, obligations, responsibilities, rights and expectations 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 insurers legal counsel) on their legal effect and enforceability.

4.4.2. An insurer 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 timely renegotiation and renewal to enable the insurer 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 insurer and right of access to information on the insurer and the service provider. It should at the very least, have provisions pertaining to:

a) the scope of the outsourcing service including the rights and responsibilities of each party, well-defined and measurable performance standards for the service provider;

b) performance, operational, internal control and risk management standards defined in terms of service levels and performance targets, service, availability, reliability, stability and upgrade;

c) confidentiality and security;

d) business continuity management;

e) monitoring and control;

f) audit and inspection;

g) <u>Notification of adverse developments</u>
An insurer should specify in its agreement the type of events and circumstances that the service provider should report, in order for prompt risk mitigation measures to be taken, and notify AMBD of such developments;

h) <u>Dispute resolution</u>
An insurer should specify in its agreement the resolution process, events of default, indemnities, remedies and recourse of the parties in the agreement. It should ensure that its contractual rights can be exercised should any breach of agreement by the service provider occur;

i) Default termination and early exit

An insurer should have the right to terminate the agreement should there be any default, or under circumstances where:

(i) the service provider undergoes a change in ownership;
(ii) the service provider becomes insolvent or goes into liquidation;
(iii) the service provider goes into receivership or judicial management whether in Brunei Darussalam or elsewhere;
(iv) there has been a breach of security or confidentiality; or
(v) there is an obvious 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 agreement. Other provisions should also be set to ensure a smooth transition when the agreement is terminated or amended. When the agreement involves an intra-group entity, the agreement should be legally enforceable against that entity providing the outsourced service;

j) Sub-contracting

An insurer should retain the ability to monitor and control its outsourcing when a service provider uses a sub-contractor. The agreement should contain clauses setting out the rules and limitations on sub-contracting. The clauses should make 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 insurer should ensure that the sub-contracting of any part of material outsourcing arrangements is subject to the insurer's prior approval;

k) Applicable laws

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

l) Any proprietary and customer information that has been shared with the service provider. These must remain secure at all times, and that strict controls are in place to prevent unauthorised access. The agreement must at least address –

(i) the responsibility of each party with respect to information security, including their rights to change the security procedures and requirements;
(ii) the scope of information subject to security requirements;

(iii) the party liable for any losses arising from a security breach; and
(iv) notification requirements in the event of a security breach;

m) Obligations on the service provider to allow the insurer and its external auditor, the necessary access to the premises, systems and any information or documents in relation to the outsourced activity.

4.4.3. Each agreement should be crafted 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 Brunei Darussalam.

4.5. Confidentiality and Security

4.5.1. As public confidence in insurers plays a vital role in the stability and reputation of the financial industry, it is important that an insurer is confident that the service provider's security policies, procedures and controls will enable the insurer to protect the confidentiality and security of customer information.

4.5.2. The insurer should be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. The insurer should take the following steps to ensure that the issue of confidentiality and security of customer information is addressed:

a) to agree and document the respective responsibilities of the contracting parties in the outsourcing agreements 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 insurer;

b) issues of access and disclosure of customer information provided to the service provider having regard to the insurer'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 unauthorised disclosure of the insurer's customer information to any party should be prohibited;

c) customer information disclosure 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;

d) to ensure the service provider is able to isolate and clearly identify the insurer's customer information, documents and records and assets to protect the confidentiality of the customer information, documents, records, and assets, particularly where multi-tenancy arrangements are present at the service provider. An insurer 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;

e) to 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 confidentiality, security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose confidentiality breaches in relation to customer information;

f) to ensure all outsourcing agreement contains a clause on confidentiality that bounds the service provider (and its employees) even after the arrangement has ceased; and

g) to ensure that information shared with a service provider is returned to the insurer on a timely and secure basis, and no longer resides with it once the outsourcing arrangement ceases or is terminated or after a reasonable period of time, when the information is no longer required for the intended purpose and upon approval or request by the insurer.

4.5.3. The level of security required to protect the confidentiality of customer information should be commensurate with the nature and materiality of the outsourcing arrangement. An insurer 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.

4.5.4. The insurer should notify AMBD of any unauthorised access or breach of security and confidentiality by the service provider or its sub-contractors that affect the insurer or its customers.

4.6. <u>Business Continuity Management (BCM)</u>

4.6.1. An insurer should ensure that its business continuity management preparedness is not compromised by outsourcing, in particular, of the operation of its critical systems. The insurer is expected to adopt sound practices and standards in BCM, in evaluating the impact of outsourcing on its risk profile and for effective BCM on an ongoing basis.

4.6.2. The insurer should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be

adequately mitigated such that the insurer remains able to conduct its business with integrity and competence in the event of service disruption or failure, or unexpected termination of the outsourcing, or liquidation of the service provider. These include steps to:

a) 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), recovery point objectives (RPO), and resumption operating capacities. Escalation, activation and crisis management procedures should also be clearly defined;

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. These tests would help familiarise the insurer and service provider with the recovery processes, and improve the coordination between the respective parties. The insurer should require the service provider to notify it of any test finding that may affect the service provider's performance, and any substantial changes in the service provider's BCP plans and any adverse development that could impact the service provided to the insurer; and

c) ensure there are plans and procedures to address adverse conditions or termination of the outsourcing arrangement, such that, the insurer will be able to continue business operations and that all the service provider is able to isolate and clearly identify the insurer's information, documents and records, and other assets such that in adverse conditions, all documents, records of transactions and information given to the service provider, assets of the insurer, can be either removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

d) An insurer must, at all times, ensure that it has in its possession, or can readily access, all records and information with respect to the outsourced activity necessary to allow it to operate and meet relevant legal and regulatory requirements.

4.6.3. For assurance on the functionality and effectiveness of its BCP plan, the insurer should design and carry out regular, complete and meaningful BCP testing of its plans as commensurate with the nature, scope and complexity of the outsourcing arrangement, including the risks arising from

interdependencies on the insurer. For tests to be complete and meaningful, the insurer 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. Likewise, the insurer should participate in its service providers' BCP and disaster recovery exercises.

4.6.4. The insurer 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. These may include unavailability of service provider due to unexpected termination of the outsourcing agreement, liquidation of the service provider and wide-area disruptions resulting in collateral impact on the insurer and service provider. Where the interdependency on an insurer in the financial system is high, the insurer 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.

4.6.5. The insurer should also assess and be satisfied with the adequacy and effectiveness of the service provider's BCP. The insurer should also ensure alignment of the service provider's BCP with its own BCP.

4.7. Monitoring and Control of Material Outsourced Activities

4.7.1. An insurer should establish a structure for the management and control of outsourcing. Such a structure will vary depending on the nature and extent, 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. The insurer also has to be more proactive in its relationships with the service provider to ensure that performance, operational, internal control and risk management standards levels are upheld (e.g. by having frequent meetings). The insurer should ensure that outsourcing agreements with service providers contain provisions to address their monitoring and control of outsourced activities.

4.7.2. A structure for effective monitoring and control of material outsourcing would comprise of the following:

a) a register of all material outsourcing that is readily accessible for review by the board and senior management of the insurer. 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 register should be updated promptly and form part of the oversight and

corporate governance reviews undertaken by the board and senior management of the insurer, similar to those described in paragraph 4.1;

b) 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 insurer should allocate sufficient resources to the management group to enable its staff to adequately plan and oversee the entire outsourcing effort;

c) establishment of management control groups to monitor and control the outsourced service on an ongoing basis. There should be policies and procedures to regularly monitor service delivery, confidentiality and security of customer information to gauge ongoing compliance with agreed service levels and the viability of its operations. These should be validated through the review of the service provider's auditor's report(s) or audits commissioned by the insurer;

d) regular reviews and audits to ensure outsourcing risk management policies and procedures, and these Guidelines, are being effectively complied with. These should determine the adequacy of internal risk management and management information systems established by the insurer, and any deficiency in its systems of control;

e) reporting policies and procedures. Reports on the monitoring and control activities of the insurer should be prepared or reviewed by its senior management and provided to its board. The insurer should ensure that monitoring metrics and performance data are not co-mingled with other customers of the service provider. It should also ensure that any adverse developments arising from any outsourced activity are brought to the attention of the senior management of the insurer and service provider. Actions should be taken by the insurer to review the outsourcing relationship for modification or termination of the agreement; and

f) comprehensive pre- and post- implementation reviews of new or amended outsourcing arrangements should be carried out. Comprehensive due diligence of any amended outsourcing arrangements should also be performed.

4.7.3. Insurer should report to AMBD if there are any adverse developments or non-compliance with legal obligations as per agreed in the outsourcing agreements.

4.8. Audit and Review

4.8.1. Outsourcing should not interfere with the ability of the insurer to effectively manage its activities or impede AMBD in carrying out its supervisory functions and objectives.

4.8.2. Every insurer should include, in its outsourcing agreements for material outsourcing arrangements, where relevant, clauses that allow:

a) the insurer to conduct periodic review and to obtain copies of any report and finding made on the service provider and its sub-contractors, whether produced by the service provider or its sub-contractors' internal or external auditors, or the service provider's and its sub-contractor's agents, in conjunction with the service performed for the insurer. Such periodic reports should be made available to the board and senior management;

b) AMBD, or any agent appointed by AMBD, where necessary or expedient, to exercise the contractual rights of the insurer to:

(i) access and inspect both the service provider and its sub-contractors, and obtain records and documents, of transactions, and information of the insurer 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-contractor's agents, in relation to the outsourcing arrangement.

4.8.3. Any major issues and concerns should be regularly brought to the attention of an insurer's senior management and service provider, or its board, where warranted. The insurer should review the outsourcing arrangement if the risk posed is beyond its risk tolerance.

4.8.4. Paragraph 4.8 is not applicable for outsourcing arrangements performed by a member of the group.

4.9. Outsourcing Outside Brunei Darussalam

4.9.1. The engagement of a service provider or an outsourcing arrangement or function in a foreign country exposes an insurer to country risk - economic, social and political conditions and events in a foreign country that may adversely affect an insurer. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the insurer.

In its risk management of such outsourcing, the insurer 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.

4.9.2. The insurer should also be aware of disaster recovery arrangements and locations established by the service provider in relation to the outsourcing arrangement. The risks associated with the mode of transport of physical or electronic data should also be considered.

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

a) the insurer should, in principle, enter into arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements;

b) the insurer 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. The insurer must at least commit to retrieve information readily from the service provider should AMBD request for such information. The insurer should confirm in writing to AMBD, the rights of inspecting the service provider and access to the insurer and service provider's information, reports and findings related to the outsourcing, as set out in paragraph 4.8;

c) the insurer should notify AMBD 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 insurer and AMBD set out in paragraph 4.8, have been restricted or denied.

4.10. Outsourcing Within a Group

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

4.10.2. 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 insurer, 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 insurer, and compliance with local regulatory requirements. 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 the insurer and other supervisory actions, depending on the potential impact of the outsourcing on the insurer and the financial system, or as circumstances warrant.

4.11. Outsourcing involving Cloud Services

4.11.1. Where a cloud service provider is involved in an outsourcing arrangement, an insurer should take adequate measures to mitigate any risks associated with the following:

a) data accessibility;

b) data confidentiality;

c) data integrity;

d) data sovereignty;

e) data recoverability; and

f) regulatory compliance.

4.11.2. The inherent risks involved in using cloud services are similar to the risks involved in using other outsourcing arrangements. Thus, these guidelines should apply to cloud services.

4.11.3. With regard to the insurer's ability to conduct audits and inspections pursuant to paragraph 4.4.2 (f) on the cloud service providers, the insurer may rely on third party certification or reports provided by the cloud service provider for audit. There should be adequate understanding and review of the scope of the audit, methods employed by and access to the third party (should any contact be needed for further clarification).

4.11.4. With regard to testing a cloud service provider's BCP pursuant to paragraph 4.6.2 (b), the insurer should be able to access information on the state of robustness of the controls instituted by the cloud service providers that arise from the BCP testing.

4.12. Outsourcing of Internal Audit to External Auditors

4.12.1. Where the outsourced service is the internal audit function of an insurer, the insurer should deliberate on the issue of independence, when a service provider handles multiple engagements for the insurer (e.g. internal and external audits and consulting work). From its internal audit role, it is doubtful that the service provider would criticise itself for the quality of the external audit or consultancy services provided to the insurer. Additionally, the insurer should also ensure that its service providers are capable of adequately completing engagements that involve complex and large transaction volumes. Therefore, the insurer should address such issues before outsourcing the internal audit function. Insurers should not outsource their internal audit function to the insurer's external audit firm.

4.12.2. Before outsourcing the internal audit function to external auditors, the insurer should satisfy itself that the external auditor would be in compliance with the relevant auditor independence standards of the Brunei accounting profession.

5. APPROVAL ON OUTSOURCING

The insurer is expected to perform its due diligence in accordance with these guidelines with endorsement from the board, or the board committee on the service provider appointed before submitting the application to the Authority.

Issue date: 20 Zulhijjah 1440 / 21 August 2019

APPENDIX 1: LIST OF MATERIAL OUTSOURCING

1. For the purpose these Guidelines, the following are other services that, when performed by a third party, would be regarded as outsourcing arrangements:

   (a) underwriting;

   (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 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, 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 insurer (e.g., accounting, internal audit, actuarial, compliance); and

   (n) support services related to archival, storage and destruction of data and records.

2. The following would NOT be considered material outsourcing:

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

(i) maintenance of custody account with specified custodians;

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

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

(i) sale of insurance policies by agents, and other means of distribution channel relating to those sales;

(ii) Reinsurance arrangement with reinsurers/retakaful operators;

(iii) acceptance of business by underwriting agents; and

(iv) introducer arrangements (where the insurer does not have any contractual relationship with policyholders).

(c) Arrangements that the insurer 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)