FINANCIAL INTELLIGENCE UNIT
AUTORITI MONETARI BRUNEI DARUSSALAM

GENERAL GUIDANCE PAPER
TO FINANCIAL INSTITUTIONS AND DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS
ON ANTI-MONEY LAUNDERING AND COMBATTING THE FINANCING OF TERRORISM

1. Introduction

1.1. The Criminal Asset Recovery Order, 2012 (CARO), enacted on 16 June 2012, is the main AML/CFT legislation that imposes certain obligations to implement measures to detect activities associated with money laundering and terrorism financing (ML/TF). Part II (Chapters I and II) of CARO contains a set of prescribed measures to assess and understand ML/TF risks and implement Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) preventive measures using a risk-based approach. CARO also requires Reporting Entities to determine customers that may pose high risks of ML/TF, and to apply enhanced due diligence (identification, verification and monitoring processes) to such customers.

1.2. This Paper is to assist financial institutions and designated non-financial businesses and professions, referred to as Reporting Entities. The objective of this Paper is to advise and guide Reporting Entities when developing and implementing their AML/CFT programmes in line with Part II of CARO.

1.3. This Paper is issued pursuant to Section 30(c) of CARO. Reporting Entities are expected to demonstrate compliance with the provisions of this Paper, as this will be included as part of AML/CFT supervision by Autoriti Monetari Brunei Darussalam (AMBD).

1.4. In principle, this Paper focuses on expected outcomes, and is not designed to set out how Reporting Entities should comply with expectations and legislation. It is intended to provide flexibility for Reporting Entities to determine how best they can comply when legislation gives them that option; however, some situations may not provide such options.

1.5. This paper defines the key elements of AML/CFT Programmes required by CARO and sets out in more detail in section 2 below the expected contents of the Programme. There are 5 parts to this paper as follows:

1.5.1 AML/CFT Programme Framework;

1.5.2 Risk Assessment Methodology;

1.5.3 Customer Due Diligence and Monitoring;

1.5.4 High Risk Customers; and

1.5.5 Record Keeping.

1.6. The following related guidance papers should be read in conjunction with this guidance paper:

1.6.1 Obligation to Submit a Suspicious Transaction Report (STR) under Section 15 of CARO and Section 47 of the Anti-Terrorism Order, 2011;

1.6.2 Cash Transaction Reporting, Section 16 of CARO; and

1.6.3 Obligations under the Anti-Terrorism (Terrorist Financing) Regulations, 2013.

2. AML/CFT Programme Framework

2.1 Section 22 of CARO requires Reporting Entities to develop and implement an AML/CFT programme. The AML/CFT Programme is expected to provide guidance to Reporting Entities on what constitutes as sufficient controls in addressing threats and vulnerabilities to Money Laundering and Terrorist Financing.

2.2 The following are the required elements of the AML/CFT Programme, combining the elements of section 22(1) of CARO with AMBD's expectations as to Programme management and oversight:

a) Governance: Board and Senior Management Oversight;

b) AML/CFT Compliance Officer;

c) Written Policies and Procedures;

d) Screening Procedures to ensure high standards when hiring employees;

e) AML/CFT Training; and

f) Independent AML/CFT Auditing.

2.3 The size and scope of the AML/CFT Programme should be appropriate to the size, business model and complexity[1] of Reporting Entities. Less complex Reporting Entities would have simpler programmes in place, whereas more complex Reporting Entities may need to implement more sophisticated and extensive methods to their programmes.

2.4 Financial groups that own subsidiaries that are Reporting Entities should have a consolidated AML/CFT Programme that enables the financial group to exercise appropriate oversight over its Reporting Entities and other subsidiaries to ensure consistent assessment of ML/TF risk and implementation of controls. If Reporting Entities have foreign subsidiaries or branches, Reporting Entities must include provisions in their programmes that extend their AML/CFT oversight to such operations.

a) Governance: Board and Senior Management Oversight

2.5 The Board of Directors, or any equivalent governing officer or body of a branch of a foreign branch (any and all of which are referred to herein as the "Board") of the Reporting Entities is expected to conduct oversight over the effective implementation and operation of the AML/CFT Programme.

2.6 Senior management is responsible for implementing the AML/CFT Programme. The Board and Senior Management should know and understand the Reporting Entity's (or group of Reporting Entities) organisational structure and the risks that it poses. If necessary, Board oversight may be delegated to a Board committee such as the Audit Committee.

[1] The level of complexity of an institution is based on the customer profiles, products and services, the size and business model of the institution, financial and accounting information, and delivery channels used for its products and services.

2.7 The Board should receive regular reports from senior management and the Compliance Officer on matters relating to ML/TF risks, compliance with the AML/CFT legislation and the relevant elements of this Guideline. The Board should also receive reports from independent audits of the overall effectiveness of their AML/CFT Programme.

2.8 In the absence of a complex governance structure, as is the case for smaller Reporting Entities, such Reporting Entities should demonstrate how the management exercises effective control over the process.

b) AML/CFT Compliance Officer

2.9 Reporting Entities are required by Section 21 of CARO to designate a compliance officer at management level to be responsible for the implementation of the Programme and ongoing compliance with CARO. The compliance officer will also be the contact person between the FIU and the reporting entity for AML/CFT purposes.

2.10 The Compliance Officer should have a direct reporting line to the Board for oversight purposes. In the case of smaller Reporting Entities (e.g. family-owned businesses), the Compliance Officer should otherwise report to (administratively) or be a member of senior management or be the beneficial owner. Compliance Officers must be provided with adequate staff and resources to accomplish their mandate.

2.11 Reporting Entities should ensure that the Compliance Officer has clear and documented responsibility and accountability for the content, design and implementation of the Reporting Entities' Programmes. In particular, the mandate should include accountability for:

2.11.1 Developing and implementing the assessment of inherent ML/TF risks (as specified under section 3 of this Paper on Risk Assessment Methodology), being satisfied that new products, new technology, services and business acquisitions are subjected to timely inherent risk analysis, and appropriate measures are developed to control identified risks while keeping such assessment and processes up to date;

2.11.2 Being satisfied that systems resources, including systems to identify and report suspicious transactions, are sufficient;

2.11.3 Ensuring AML/CFT policies and procedures are up to date and approved by senior management and/or the Board;

2.11.4 Reporting to the Board and/or senior management on relevant information about suitability and concerns of their AML/CFT programmes, and ensuring that systems and procedures that generate information used in reports to Board and/or senior management are adequate, appropriate and generate accurate information;

2.11.5 Ensuring that AML/CFT training programmes are in place as required by the policies;

2.11.6 Filing of CTRs and STRs with the FIU, according to the guidance issued on obligations for CTR and STR submission; and

2.11.7 Ensuring compliance with the Anti-Terrorism (Terrorist Financing) Regulations, 2013.

2.12 In cases where Reporting Entities delegate or assign AML/CFT duties to other individuals, or outsources some elements of their AML/CFT programme to third parties that do not report to the Compliance Officer, the reporting entity should take reasonable measures to be satisfied that such elements are implemented effectively. This could include receiving regular reports from such other individuals or third parties on how the measures were implemented;

2.13 Responsibility for the implementation of the AML/CFT programme requires that the Compliance Officer has:

2.13.1 Comprehensive working knowledge of ML/TF risks and controls of the reporting entity and AML/CFT regulatory requirements imposed by law or the AMBD;

2.13.2 A broad understanding of the operations of the reporting entity, its obligations and weaknesses; and

2.13.3 Appropriate professional qualifications, experience and leadership skills.

2.14 Larger Reporting Entities, such as banks and finance companies, are expected to establish separate units or departments for compliance functions. However, depending on the scale and nature of business of certain Reporting Entities, it is acceptable to have:

2.14.1 a designated officer for the compliance function provided that there are sufficient resources to conduct the responsibilities of a Compliance Officer.

2.14.2 the Compliance Officer or compliance function outside Brunei Darussalam provided that the Compliance Officer or compliance function are adequately trained in the domestic requirements and regulatory expectations, and where applicable, available for on-site inspections whenever conducted by AMBD.

2.15 Reporting Entities are expected to demonstrate the effectiveness of the approach to the compliance structure adopted commensurate with the size and complexity of the Reporting Entities.

c) Written Policies and Procedures

2.16 Written policies and procedures ensure that all employees and the Board understand their obligations and responsibility for implementing them. The scope of these policies and procedures should cover all the principal elements of an AML/CFT Programme outlined in this guideline and should be proportionate to the size and complexity of their operations.

2.17 The policies and procedures should also contain the Reporting Entity's assessment and how it addresses the entity's risk exposure to the misuse of technology and technological developments. Specific attention should be given to payment systems, including those which can be accessed by customers; in other words, technology which may enable customers to bypass or avoid measures to conduct identification verification.

d) Screening Procedures to ensure high standards when hiring employees

2.18 Reporting Entities should implement processes to ensure that all new recruitment of staff, officers, and senior management are subject to thorough screening including business reference checks, background checks for any criminal activity or other regulatory sanctions whether in Brunei Darussalam or elsewhere.

e) AML/CFT Training

2.19 Reporting Entities should provide all staff, officers, and senior management with training on ML/TF risks and vulnerabilities, and regulatory requirements of AMBD, appropriate to their roles and responsibilities. It is recommended that a standard training programme be established, supplemented by specific training modules for individuals associated with higher or special risks as follows:

2.19.1 The Board should be trained in understanding management's obligations so they can monitor them;

2.19.2 The Compliance Officer and compliance function should be trained in specialized vulnerabilities (correspondent banking relationships, high risk customers, enhanced due diligence, STR determination, etc.);

2.19.3 Those responsible for independent auditing should be trained on AML/CFT obligations and what constitutes effective implementation of measures; and

2.19.4 Front line staff should be trained to identify, assess and control the risks when dealing directly with customers.

f) Independent AML/CFT Auditing

2.20 CARO section 22(1)(e) requires Reporting Entities to have independent audit arrangements in place to review and verify compliance with and effectiveness of measures taken in accordance with CARO. The audit process should be operated independently from the direct oversight of management and the Compliance Officer, and be capable of providing the senior management and the Board with an impartial opinion on whether the AML/CFT Programme provides for an appropriate risk assessment process, compliance with relevant AML/CFT legislation, and that control measures are in place and are being operated effectively.

2.21 Such audit can be conducted by internal auditors who can take responsibility for including the AML/CFT Programme in the Reporting Entity's regular internal audit programme. Alternatively, Reporting Entities can appoint an external auditor to carry out this obligation.

2.22 Reporting Entities that lack internal or external auditors may have the audit carried out by another suitably qualified person provided that such person is appropriately independent from those responsible for implementing the controls and those responsible for reviewing them. If Reporting Entities outsource the independent audit of the AML/CFT programme, it should ensure the auditor is qualified to undertake the audit and should set out the requirements of the audit in a written contract.

3. Risk Assessment Methodology

3.1 A robust AML/CFT programme requires a Reporting Entity to identify and analyse ML/TF risks present within the entity and apply control measures that are commensurate with the identified risks.

3.2 Reporting Entities should clearly specify factors used in their risk assessment methodology in determining their ML/TF risks. The different risk factors that may be used in assessing ML/TF risks are as follows:

a) Customer risks;

b) Business relationship risks;

c) Product or service risks (including the risk of misuse of technological developments)

d) Delivery channel risks; and

e) Geographic location risks.

3.3 The outcome of the ML/TF risk methodology adopted should be a rational, well-organized and sufficiently documented inherent risk analysis that takes into account the risk factors and enables Reporting Entities to identify their high risk customers as required by CARO section 9(a). In addition, Reporting Entities should take into account the threats and vulnerabilities of sectors in which they operate, as set out in the National Risk Assessment.

a) Customer Risk

3.4 This is risk associated with types of customers that buy or use the Reporting Entity's products and services, and includes persons acting as guarantors of such customers where applicable. Categories of customers or guarantors that may indicate an inherently higher risk could include those who:

3.4.1 Conduct their business relationship or transactions in unusual circumstances for which there is no reasonable economic purpose;

3.4.2 Deal in firearms, weapons, restricted material or goods subject to export or import restrictions;

3.4.3 Operate in a structure or with business relationships that make the identification of the ultimate beneficial owner(s) difficult or complex, such as:

(i) Corporations with the ability to issue bearer shares;

(ii) Corporations incorporated in jurisdictions that are not connected to the objectives of the business relationship; or

(iii) Trusts set up in offshore jurisdictions;

3.4.4 Operate cash (and cash equivalent) intensive businesses including:

(i) Money services business, e.g. remittance, currency exchange businesses, bank note traders, cash couriers or other businesses offering money transfer or movement facilities);

(ii) Businesses that, while not normally cash-intensive, generate substantial amounts of cash for certain lines of activity;

3.4.5 Are dealers or traders in high value goods such as works of art, high-end automobiles and auction houses.

3.4.6 Are charities or other non-profit organisations that are engaged in providing financial support to persons of low income in foreign countries; and

3.4.7 Are politically exposed persons (PEPs)- refer to section 5 on high risk customers

3.5 Insurance and takaful companies are expected to consider the beneficiaries of life insurance and family takaful policies as risk factors in determining the overall ML/TF risks associated with their customers. Generally, this will involve screening the names of beneficiaries as if they were customers and assessing any identified risks that may be associated with them.

b) Business relationship risk

3.6 This is risk associated with the customer's stated purpose in dealing with the reporting entity. Categories of business relationships that may indicate a higher risk could include:

3.6.1 Intermediary structures, such as holding companies, numbered companies or trusts, that have no apparent business purpose or that make beneficial owners difficult to identify;

3.6.2 Accountants, lawyers or other professionals holding collective funds accounts where the underlying beneficial ownership of the funds may be difficult to verify; and

3.6.3 Use of the Reporting Entity's products or services by customers of customers, for example, customers of correspondent banks.

c) Product/Service Risk

3.7 This is risk associated with products and services (including new products and services) that enable customers to move funds, and includes the risk of misuse of technology and technological developments. Categories of products and services that may indicate a higher risk could include:

3.7.1 Specific technologies such as blockchain, virtual currency, prepaid cards, and other vehicles that can be used to store, record, or transfer value by others outside the oversight of the Reporting Entities;

3.7.2 Deposit-taking, especially cash, and insurance products that allow large one-time or regular payments, pre-payments or deposits, to be made and subsequently withdrawn from deposit or deposit-like accounts;

3.7.3 Cash values, early cash surrender and loan provisions, and provisions for deposit, accumulation and withdrawal of funds with relative ease and speed;

3.7.4 Trade finance services where –

(i) The Reporting Entities are not able to assess whether the value of goods or services being imported or exported are reasonable; or

(ii) Reporting Entities confirm, advise or make payments under letters of credit for purposes of their customers' buying or selling goods internationally.

3.7.5 Syndicated loans, where the Reporting Entity is a member of the syndicate led by a bank (whether domestic or foreign) that has the primary customer relationship with the borrower;

3.7.6 Credit accounts in respect of which large credit balances are allowed to be maintained, for example, some credit and corporate card products;

3.7.7 Payable-through accounts that permit customers of a foreign bank (respondent) to draw drafts (or cheques) on Brunei-based accounts; and

3.7.8 International bank payments through postal or courier services, and similar international commercial payment services.

d) Delivery Channel Risk

3.8 This is risk associated with how Reporting Entities' products or services are delivered to customers including services delivered in a non-face-to-face manner. Categories of delivery channels that may indicate a higher risk could include:

3.8.1 Information provided by intermediaries or other third parties that may not be subject to AML/CFT laws and measures and/or who are not adequately supervised;

3.8.2 Syndicated loans; and

3.8.3 The Internet, telephone and mailing services when used as a complete substitute for face-to-face interaction with the customer in delivering services.

3.9 Section 5(7) of CARO requires Reporting Entities to take adequate measures to address ML/TF risk in the event that the customer is not physically present for the purposes of identification. Please refer to paragraph 4.7 below for more detailed information.

e) Geographic location risk

3.10 This is risk associated with places in or to which Reporting Entities have branches or subsidiaries in, which may mitigate or elevate the risk. Categories of countries or jurisdictions that may indicate a higher risk include those that are:

3.10.1 Subject to Brunei Darussalam or other national sanctions, embargoes or similar actions;

3.10.2 Subject to United Nations Security Council (UNSC) sanctions (refer to guidance on Obligations under the Anti-Terrorism (Terrorist Financing) Regulations, 2013);

3.10.3 Identified by credible sources as providing funding or support for terrorist activities or the proliferation of weapons of mass destruction;

3.10.4 Identified by credible sources as having significant levels of corruption or other criminal activity;

3.10.5 Listed by the Financial Action Task Force (FATF) as having systemic deficiencies in implementing AML/CFT measures, or subject to countermeasures applied by the FATF; and

3.10.6 Subject to domestic laws or regulations that prohibit or restrict access to customer information, including beneficial ownership information.

4. Customer Due Diligence and Monitoring

a) Account Opening and Identification of Customers

4.1 Reporting Entities must have account opening and customer identification processes in place that implement the applicable or requisite elements of Customer Due Diligence (CDD) as set out under Sections 4, 5 and 6 of CARO. For the purposes of this paper, AMBD considers guarantors as customers.

4.2 The names of all customers must be their true names and must be determined in the following circumstances:

4.2.1 When establishing business relations with a customer as defined in CARO;

4.2.2 When carrying out any transaction in an amount greater than B$15,000 or the equivalent amount in a foreign currency, whether the transaction is carried out in a single transaction or in multiple transactions that appear to be linked;

4.2.3 Where there is a suspicion of ML/TF, which applies to all business relationships, transactions and related matters regardless of thresholds, exemptions or other exceptions; and

4.2.4 Where the reporting entity has doubts about the accuracy and adequacy of previously obtained identification data.

b) Determining Beneficial Ownership of Customers

4.3 Under Section 5(2) of CARO, Reporting Entities must determine the beneficial owner(s) of customers that are legal persons or legal arrangements. “Beneficial owner” is defined in CARO as:

4.3.1 A natural person who ultimately owns or controls the rights to and/or benefits from property, including the person on whose behalf a transaction is conducted;

4.3.2 A natural person who exercises ultimate effective control over a legal person or legal arrangement;

4.3.3 A natural person is deemed to ultimately own or control rights to or benefit from property when that person –

(i) Owns or controls, directly or indirectly, including through trusts or bearer share holdings for any legal entity, 25 percent or more of the shares or voting rights of the entity; or

(ii) Otherwise exercises control over the management of the entity.

4.4 It is important for Reporting Entities to understand that where there is a chain of ownership of legal persons or trusts between the customer and the ultimate beneficial owner(s), it is necessary to establish the names and respective beneficial ownership of all such legal persons

or arrangements, until there are no further legal entities or trusts in the chain and the Reporting Entity is able to arrive at the name(s) of the natural person(s) who is/are the beneficial owner(s). For complex ownership structures, this may involve extensive research before the name(s) of the beneficial owner(s) is/are established.

4.5 Where a Reporting Entity is in doubt about whether a natural person is a beneficial owner, or where there is no beneficial owner exerting control, the Reporting Entity should verify the identity of the person who is the senior managing official of the customer.

4.6 Once the beneficial owner(s) of a client has been determined, Reporting Entities are expected to determine if such beneficial owner(s) is (are) Politically Exposed Persons (PEP).

c) Reliance on Intermediaries and Third Parties for Customer Identification Process

4.7 Section 5(3) of CARO authorizes Reporting Entities to rely on intermediaries and third parties when obtaining customer identification information, but Reporting Entities retain the responsibility for ensuring the information obtained complies with the requirements of CARO, and for taking compensatory measures if that is not the case. Reporting Entities should also take measures to ensure that such intermediaries and third parties are adequately regulated, supervised or monitored for AML/CFT obligations.

4.8 Reporting Entities should ensure they understand the difference between relying on intermediaries or other third parties to implement their customer identification and verification requirements, and using an agent for such purposes. An agent is considered as an extension of the Reporting Entity itself, and thus the Reporting Entity is responsible for ensuring that agents apply the same requirements as set out in the Reporting Entity's Programme.

4.9 A Reporting Entity may only rely on such intermediaries and third parties in the following circumstances:

4.9.1 When the Reporting Entity is satisfied that the intermediary or third party:

(i) is capable of supplying the necessary customer information upon request and without delay;

(ii) is an entity regulated for AML/CFT requirements, or is established in a country where it is subject to AML/CFT requirements consistent with FATF standards; and

(iii) have adequate measures in place to comply with the above requirements.

4.9.2 When there is no suspicion of ML or TF. If the Reporting Entity files an STR on the customer, the Reporting Entity may no longer rely on the source of information obtained from intermediaries and third parties, and must obtain customer information directly; and

4.9.3 If customer information is obtained immediately upon account opening or the commencement of the relationship. If the Reporting Entity receives such information after a certain period of time beyond immediate, i.e. 2 or 3 working days, then the

Reporting Entity may no longer rely on the source of information obtained from intermediaries and third parties and must obtain customer information directly.

4.10 Reporting Entities should have a policy of having written agreements with any intermediaries or third parties on whom reliance is placed as authorized by Section 5(3) of CARO. The agreements should ensure that Reporting Entities can comply with the requirements of CARO and should be terminated where counterparties are unable to fulfil the scope and timeliness of their obligations.

d) Information to be obtained on customers

4.11 Section 6 of CARO sets out the information that Reporting Entities must collect, verify and retain on each of their customers. The legal requirements are set out as follows:

4.11.1 For customers that are individuals, their:

(i) full name,

(ii) home address,

(iii) identity card number or any official document indicating identity, and

(iv) date and place of birth.

An official document is a document bearing the photograph of the person and issued by a government or a government agency, including a foreign government;

4.11.2 For customers that are legal persons:

(i) Their registered address and proof of incorporation, via a recent certificate of incorporation confirming the current existence of the legal person;

(ii) Information on persons who have authority to bind customers who are legal entities; and

(iii) Verification of the identities of the directors, as well as their status as directors being confirmed within the certificate of incorporation or any other document authenticating the existence of the legal person.

4.11.3 For customers that are legal arrangements (trusts) Reporting Entities must:

(i) obtain proof of the existence of the trust;

(ii) determine if the beneficiary of the trust property, or any other person with control over the trust property, including the trustee(s), the settlor, or the protector, is a PEP; and

(iii) obtain information on all persons who have authority to bind the trust.

4.11.4 For beneficial owners of legal persons and legal arrangements: the name of the person should be recorded along with supporting information clearly establishing the link between the person and the customer of which he or she is the beneficial owner. Reporting entities must also determine if the beneficial owners are PEP; and

4.11.5 With respect to each customer: obtain sufficient information about the nature and business of the customer that will permit the Reporting Entity to comply with any AML/CFT requirements imposed by AMBD relating to such customers. This expectation is linked to the requirements of Section 12 of CARO relating to monitoring obligations.

4.12 The CDD obligations also apply to Reporting Entities when dealing with anyone who is authorized to act on behalf of a customer. Such persons must be subject to the Reporting Entity's identification and verification processes.

e) Information to be obtained when issuing wire transfers

4.13 Section 6(2) of CARO sets out information that must be obtained by Reporting Entities (mostly by banks and financial institutions) when processing domestic or international wire transfers, including transfers bundled in a batch file. When a person attempts to conduct a wire transfer but does not have an established business relationship with the Reporting Entity, the Reporting Entity must apply the identification measures prescribed under Sections 5 and 6 of CARO beforehand to such customer.

f) Customer Identification and Account Opening for Cross-Border Correspondent Banking Relationships

4.14 Section 10 of CARO imposes customer identification, verification and record-keeping obligations on Reporting Entities that are financial institutions seeking to establish cross-border correspondent banking relationships (CBR) with foreign financial institutions, referred to in CARO as respondent institutions.

4.15 Reporting Entities should keep records of the foreign financial institutions with which they have SWIFT key relationships. Such relationships should be kept to a minimum and be subject to clearly documented policies supporting the retention of SWIFT keys with foreign financial institutions. A policy should also be in place that requires consideration be given to terminating open SWIFT keys that remain unused for extended periods of time.

4.16 Before establishing a correspondent banking relationship with any foreign financial institution, Reporting Entities should ensure that they establish an agreement in writing with such foreign financial institution. The agreement should address:

4.16.1 The nature and business of the respondent institution. Reporting Entities should obtain documents, reports and other materials verifying these activities;

4.16.2 The ability of the Reporting Entity to obtain information about the AML/CFT internal controls of the respondent institution on a timely basis;

4.16.3 The laws of the jurisdiction where the respondent institution is chartered or incorporated that authorises the respondent institution to access official documentation supporting this information. Reporting Entities are prohibited from dealing with shell banks – therefore the agreement should clearly confirm that the respondent institution has a physical presence where it is chartered or incorporated,

unless it is part of a regulated services group that is subject to effective consolidated supervision; and

4.16.4 Confirmation that the respondent institution has measures in place to prevent its accounts from being used by shell banks.

4.17 Payable-through accounts expose Reporting Entities to the ML/TF risks that may be associated with customers of respondent institutions, specifically if such institutions apply inadequate monitoring to their customers' transactions. Therefore, if the correspondent banking relationship agreement includes the provision of payable-through accounts, Reporting Entities should ensure that the respondent institution applies adequate domestic AML/CFT measures and is subject to AML/CFT supervision. This should include being satisfied that such measures are, at a minimum, generally consistent with Sections 5 to 10 of CARO.

g) Timing of Implementation of Customer Identification and Verification Processes

4.18 Section 8 of CARO requires customer identification and verification measures to be implemented before establishing an account or a business relationship. However, there are certain circumstances where certain Reporting Entities may complete the verification of the identity of customers as soon as reasonably practicable after the commencement of the business:

4.18.1 For Securities dealers: when processing the purchase or sale of shares listed on a stock exchange for a new customer, where the verification of identity might result in financial disadvantage to the customer due to changes in market prices. In these circumstances, the securities dealer may only process the purchase, or deposit the proceeds of the sale, to the customer's account. No further transactions may be undertaken by the customer until the verification process is complete; and

4.18.2 For Insurance and Takaful companies: when issuing life insurance or family Takaful policies, provided that the total premiums to be paid by the customer over the lifetime of the policy do not exceed $15,000. In these circumstances, the insurance or Takaful company shall complete the verification on the identity of the customer within 10 business days of issuing the policy to the customer.

h) Monitoring and Ongoing Due Diligence

4.19 Section 12 of CARO requires Reporting Entities to apply special measures to certain business relations and transactions.

4.20 Reporting Entities are required to pay special attention to:

4.20.1 all complex, large unusual transactions and all unusual patterns of transactions that have no apparent economic or visible lawful purpose; and

4.20.2 business relations and transactions with persons, including legal persons and arrangements, from or in countries that do not or insufficiently apply the relevant international standards to combat ML/TF.

4.21 Reporting Entities, in particular financial institutions, are expected to have in place adequate transaction monitoring systems that enable the detection and assessment of transactions that may be, or appear to be, unusual or suspicious. Such systems should facilitate the Reporting Entity with a holistic view of customers' past transactions, customers' normal patterns of activities, and customer/business profiles that are accurate and updated.

4.22 Reporting Entities should have processes in place to review whether the transactions flagged by the transaction monitoring system are suspicious before reporting to the FIU.

4.23 Reporting Entities should also consider integrating customer identification and monitoring systems with the systems required to comply with the implementation of targeted financial sanctions. Please refer to guidance paper on obligations under the Anti-Terrorism (Terrorist Financing) Regulations, 2013.

4.24 An effective transaction monitoring system should take into account the specific risks associated with the institution's risks and context. Reporting Entities should demonstrate the adequacy and effectiveness of the system commensurate with the size, complexity and risk exposure of the Reporting Entities.

i) Circumstances when Reporting Entities may not do business with customers

4.25 Section 11 of CARO prohibits Reporting Entities from establishing accounts, issuing policies or opening business relationships with customers if they are unable to fulfill the requirements of Sections 5 to 10 of CARO with respect to any customer.

4.26 In addition, Reporting Entities are required to consider filing an STR, if appropriate. Reporting entities are expected to develop policies and procedures on the circumstances considered appropriate for this purpose.

5. High Risk Customers

5.1 Section 9 of CARO obliges Reporting Entities to exercise enhanced identification, verification and ongoing due diligence procedures with respect to their high-risk customers. This requires Reporting Entities to determine which of their customers may pose high risks of ML/TF and there should be a process to categorise customers as high risk if any of their customers meet the high-risk criteria and that enhanced measures are applied to these high risk customers.

5.2 Reporting Entities are expected to be able to demonstrate that enhanced procedures applied to such customers are demonstrably more extensive, intrusive, detailed and/or in depth than standard measures applied to customers that are not high risk.

5.3 Additional procedures should apply to high risk customers from high risk countries and are Politically Exposed Persons (PEPs), described further below.

a) High-Risk Countries

5.4 Reporting Entities should ensure that the following countries and jurisdictions are treated as high risk when assessing risks associated with customers, business relationships, products, services and delivery channels:

5.4.1 Countries and jurisdictions that are not members of the FATF or the Asia/Pacific Group (APG) or one of their affiliates[2];

5.4.2 Countries and jurisdictions that are subject to a call by the FATF or the APG for countermeasures; and

5.4.3 Countries and jurisdictions, including members of the FATF or one of its affiliates, that are being monitored from time to time by the FATF or otherwise identified by the FATF as having strategic deficiencies in their AML/CFT regimes.

5.5 Reporting Entities are expected to have processes to determine and monitor which countries are members of the FATF and its affiliates, and to monitor the FATF's and APG's websites (and other relevant FATF affiliates' websites) for periodic updates on countries and jurisdictions specified in items 5.4.2 and 5.4.3 above.

[2] As a member of the APG, which is affiliated with the FATF, Brunei Darussalam has agreed to comply with the measures applied by the APG and FATF from time to time.

b) Politically Exposed Persons (PEPs)

5.6 Section 9(b) of CARO requires Reporting Entities to determine which of their customers and their beneficial owners are PEPs, and to obtain the approval of senior management to establish or continue a business relationship, depending on when the customer or beneficial owner is identified as a PEP. PEPs are defined in CARO as follows:

5.6.1 any person who is or has been entrusted with a prominent public function including, but not limited to a head of state or of government, a senior politician, a senior government, judicial or military official;

5.6.2 any person who is or has been an executive of a state- owned company;

5.6.3 any person who is or has been a senior political party official;

5.6.4 any person who is or has been entrusted with a prominent function by an international organization; and

5.6.5 any immediate family member or close associate of such persons.

5.7 Reporting Entities should use the definition of "relative" and "associate" as defined in CARO for the purposes of complying with the "immediate family member" and "close associate" definition.

5.8 It is important for Reporting Entities to note that the positions contained in the PEP definition are not limited to Brunei Darussalam but also apply to other countries. It is also important to note that the definition of PEP applies to any position held by the person in the past. However, for customers who have been but are no longer entrusted with the prominent public function, Reporting Entities should demonstrate they have adequately assessed the ML/TF risk that customer (including immediate family members and close associates) continues to present.

5.9 The head of an international organisation is the main person leading the organisation, for example a president, chairperson, managing director or chief executive officer. An international organisation is an organisation set up by the governments of more than one country. If the organisation was established by means of a formally signed treaty or agreement between different governments, then it is an international organisation for the purposes of compliance with CARO. The law in Brunei Darussalam and other countries recognizes the existence of international organisations, which goes beyond trade and financial related organisations. Such organisations may also be resident in more than one particular country, examples of which include but are not limited to:

> The United Nations (including its various organs, funds, programmes, agencies and subsidiaries), ASEAN, European Union, Organisation for Islamic Cooperation, Financial Action Task Force, Asian Development Bank, Asia Pacific Economic Cooperation, World Bank, and International Monetary Fund.

5.10 Given the substantial number of such positions around the world, it is important that the measures Reporting Entities take to determine if a person is a PEP are realistic and

comprehensive. Reporting Entities are recommended to adopt either one of the following processes, if not both, to determine if customers or beneficial owners are PEPs:

5.10.1 Obtain sufficient information from the customer or the beneficial owner to be able to make the determination. This should also include information about the present and previous primary employments or business activities of customers and beneficial owners; or

5.10.2 Subscribe to a third-party service that contains a PEP database, for the purposes of searching for the names of customers or beneficial owners and gathering the supporting information. Reporting Entities should ensure that the chosen third-party service is capable of identifying all PEPs, as well as heads of international organisations, and their relatives and close associates.

5.11 Reporting Entities must have a formal process in place to make a determination, following the collection of information, on whether a person or beneficial owner is a PEP or a relative or a close associate of a PEP. For Insurance and Takaful companies, this requirement extends to beneficiaries (individuals or the beneficial owners of legal persons or the property in legal arrangements) designated by the holders of life insurance policies or family takaful products.

5.12 In addition to obtaining the customer due diligence information as required under Section 6 of CARO, Section 9(b) (ii) requires Reporting Entities to take all reasonable measures to identify the source of wealth, funds and other assets of customers identified as PEPs. The following are considered to be reasonable measures for enhanced due diligence:

5.12.1 Obtaining additional information on the customer and beneficial owner from their person or any reliable third-party PEP database, such as:

(i) employment history of the customer, including salaries and income associated with the positions held; and

(ii) total value of all assets held by the customer, both inside and outside Brunei Darussalam, to assess the reasonableness of such customer being able to accumulate such assets based on the salaries and other income associated with the positions held;

5.12.2 Obtaining approval from senior management before establishing a new business relationship or continuing an existing business relationship with the customer; and

5.12.3 Considering the relationship between the customer or beneficial owner identified as a PEP and any of their close associates and relatives, and assess the financial impact of such relationships.

5.13 Where the information collected (either from the person or a third-party database) suggests that the customer or beneficial owner is a PEP, Reporting Entities should collect additional information on the relatives and close associates of such PEPs, and conduct a search of its customer database or files to determine if services may already be provided to such persons. If this is the case, such persons must also be treated as PEPs, and the prescribed measures above must be applied to their accounts and relationships.

6. Record Keeping

6.1 Section 14 of CARO requires Reporting Entities to establish and maintain various types of records according to the types of customers and transactions. These records must be made available upon request to AMBD and to law enforcement agencies, pursuant to regulations or court orders or similar measures. Where such records are to be submitted to law enforcement agencies, Reporting Entities should ensure that such records are made available on a timely basis.

6.2 Reporting Entities should retain transaction and customer records for a period of at least 7 years from the date of completion of the transaction or upon which action was last taken. In the case of records related to customers' closed accounts, the records must be retained for at least 7 years from the date the accounts were closed.

6.3 In situations where the records are subject to ongoing investigations or prosecution in court, they shall be retained beyond the stipulated retention period until it is confirmed by the relevant agencies, that such records are no longer needed.

Date: 11 July 2019