Sector-Specific Guidance Notes for Corporate Service Provider Business

These sector-specific guidance notes should be read in conjunction with the main guidance notes for AML/ATF regulated financial institutions on anti-money laundering and anti-terrorist financing.

Table of Contents

Introduction…….3
Status of the guidance…….5
Senior management responsibilities and internal controls…….6
Risk-based approach for RFIs conducting corporate service provider business….9
ML/TF risks in the provision of corporate services
Customer due diligence……10
Purpose and intended nature of the customer's business relationship with the RFI
Source of wealth and source of funds
Definition of customer in a corporate service provider business context
Definition of beneficial owner in a corporate service provider business context
Obtaining and verifying customer identification information
Obtaining and verifying beneficial owner information
Timing of customer due diligence
Previous due diligence and reliance on third parties
Refusing or terminating corporate service provider business
Customer transactions involving cash or bearer instruments
Applicability of simplified due diligence to corporate service provider business
Enhanced due diligence for corporate service providers
International sanctions…….23
On-going monitoring……..……...……24
Suspicious activity reporting……..……..26
Failure to report and tipping-off offenses
Employee training and awareness……..……..28
Record-keeping……..…… 29
Risk factors for corporate service provider business……...…….. 30
Customer risk
Products and services risk
Transaction risk
Delivery channel risk
Third party risk
Geographic risk

ANNEX VI

SECTOR-SPECIFIC GUIDANCE NOTES FOR CORPORATE SERVICE PROVIDER BUSINESS

Introduction

VI.1 This annex sets forth guidance on AML/ATF obligations under the Acts and Regulations of Bermuda that are specific to corporate service provider (CSP) business.

VI.2 Under Regulation 2(2)(i) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (the Regulations), persons carrying on corporate service provider business within the meaning of the Corporate Service Provider Business Act 2012 are designated as anti-money laundering and anti-terrorist financing (AML/ATF) regulated financial institutions (RFIs).

VI.3 Under section 2(2) of the Corporate Service Provider Business Act 2012, corporate service provider business means the provision of any of the following corporate services for profit:

a. Acting as a company formation agent, or agent for the establishment of a partnership;
b. Providing nominee services, including (without limitation) acting as or providing nominee services;
c. Providing administrative and secretarial services to companies or partnerships including one or more of the following services:

    i. Providing a registered office;
    ii. Providing an accommodation, correspondence or administrative address;
    iii. Maintaining the books and records of a company or partnership;
    iv. Filing statutory forms, resolutions, returns and notices;
    v. Acting as or fulfilling the function of or arranging for another person to act as or fulfil the function of a person authorised to accept service of process on behalf of a company or partnership or to accept any notices required to be served on it;
    vi. Acting as or fulfilling the function of or arranging for another person to act as or fulfil the function of a director, officer, secretary, alternate, assistant or deputy secretary of a company or an officer of a partnership;
    vii. Keeping or making any necessary alteration in the register of

members of a company in accordance with section 65 of the Companies Act 1981;

d. The performance of functions in the capacity of resident representative under the
Companies Act 1981, Exempted Partnerships Act 1992 and the Overseas Partnerships Act 1995; and
e. Providing any additional corporate or administrative services as may be specified in regulations.

VI.4 The references in paragraph VI.3 to companies and partnerships are to client companies and partnerships wherever they are incorporated or otherwise established, and to any similar or equivalent structures or arrangements, however they are named.

VI.5 All RFIs must comply with the Acts and Regulations, and with the main AML/ATF guidance notes issued by the BMA.

VI.6 Schedule 1, section 3 of the Corporate Service Provider Business Act 2012, as amended in 2014, states that in determining whether a corporate service provider is conducting its business in a prudent manner, the Bermuda Monetary Authority (BMA) will take into account any failure to comply, among other things, with:

- The Proceeds of Crime Act 1997;
- The Anti-Terrorism (Financial and Other Measures) Act 2004;
- The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008; and
- International sanctions in effect in Bermuda.

VI.7 For the purposes of these guidance notes, the terms “AML/ATF regulated financial institution” and “RFI” should be understood to include persons conducting the corporate service provider business described in paragraph VI.3. The term “corporate service provider business” should be understood to include any and all of the activities described in paragraph VI.3.

VI.8 RFIs conducting corporate service provider business should read these sector specific guidance notes in conjunction with the main guidance notes for AML/ATF regulated financial institutions on anti-money laundering and anti-terrorist financing. This annex supplements, but does not replace the main guidance notes.

VI.9 Portions of this annex summarise or cross-reference relevant information that is contained in detail in the main guidance notes. The detailed information in the main guidance notes remains the authoritative guidance.

VI.10 Portions of this annex include sector-specific information, such as risk indicators that are particular to corporate service provider business. This sector-specific information should be considered as supplementary to the main guidance notes.

Status of the guidance

VI.11 Approved by the Minister of Justice, these guidance notes are issued by the BMA under Section 5(2) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA Act 2008), Section 49A of the Proceeds of Crime Act 1997 (POCA 1997), and Section 12B of the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA 2004).

VI.12 These guidance notes are of direct relevance to all senior management, inclusive of the Compliance Officer, and to the Reporting Officer. The primary purpose of the notes is to provide guidance to those who set the RFI's risk management policies, procedures and controls for the prevention and detection of money laundering and terrorist financing (ML/TF).

VI.13 The Court, or the Authority, as the case may be, in determining whether a person is in breach of a relevant provision of the Acts or Regulations, is required to consider whether a person has followed any relevant guidance approved by the Minister of Justice and issued by the Authority. These requirements upon the Court or Authority are detailed in the provisions of Section 49M of POCA 1997, Regulation 19(2), Section 12(O) of, and paragraph 1(6) of Part I, Schedule I to, ATFA 2004 and Section 20(6) of the SEA Act 2008.

VI.14 When a provision of the Acts or Regulations is directly described in the text of the guidance, the guidance notes use the term **"must"** to indicate that the provision is mandatory.

VI.15 In other cases, the guidance uses the term **"should"** to indicate ways in which the requirements of the Acts or Regulations may be satisfied, while allowing for alternative means, provided that those alternatives effectively accomplish the same objectives.

VI.16 Departures from this guidance, and the rationale for so doing, should be documented, and RFIs should stand prepared to justify departures to authorities such as the BMA.

VI.17 RFIs should be aware that under section 16 (1) of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency may, in the course of enquiring into a suspicious transaction or activity relating to money laundering or terrorist financing, serve a notice in writing on any person requiring the person to provide the Financial Intelligence Agency with such information as it may reasonably require for the purpose of its enquiry.

VI.18 Detailed information is set forth in the main guidance notes, beginning with the Preface.

Senior management responsibilities and internal controls

VI.19 The AML/ATF responsibilities for senior management of an RFI conducting corporate service provider business are governed primarily by the POCA 1997, SEA Act 2008, ATFA 2004, and the supporting Regulations.

VI.20 The AML/ATF internal control requirements for RFIs conducting corporate service provider business are governed primarily by Regulations 12, 16 and 18 and 18A.

VI.21 Regulation 19 provides that failure to comply with the requirements of specified Regulations is a criminal offence and carries with it significant penalties. On summary conviction, the penalty is a fine of up to $50,000. Where conviction occurs on indictment, penalties include a fine of up to $750,000, imprisonment for a term of two years, or both.

VI.22 Section 20 of the SEA Act 2008 empowers the BMA to impose a penalty on an RFI of up to $500,000 for each failure to comply with specified Regulations. The SEA Act also provides for a number of criminal offences, including carrying on business without being registered pursuant to Section 9 of the Act.

VI.23 Under the Acts and Regulations of Bermuda, senior management in all RFIs must:

- Ensure compliance with the Acts and Regulations;
- Identify, assess and effectively mitigate the ML/TF risks the RFI faces amongst its customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Ensure that risk assessment findings are maintained up to date;
- Appoint a Compliance Officer at the senior management level to oversee the establishment, maintenance and effectiveness of the RFI's AML/ATF policies, procedures and controls;
- Appoint a Reporting Officer to process disclosures;
- Screen employees against high standards;
- Ensure that adequate resources are devoted to the RFI's AML/ATF policies, procedures and controls;
- Audit and periodically test the RFI's AML/ATF policies, procedures and controls for effectiveness; and
- Recognise potential personal liability if legal obligations are not met.

VI.24 RFIs must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF.

VI.25 An RFI must include its AML/ATF policies and procedures with its application for a corporate service provider business licence.

VI.26 Where a Bermuda RFI conducting corporate service provider business has branches, subsidiaries or representative offices located in a country or territory other than Bermuda, it must communicate its AML/ATF policies and procedures to all such entities and must ensure that all such entities apply AML/ATF measures at least equivalent to those set out in the Acts and Regulations.

VI.27 Attempts to launder money through corporate service provider business services may be carried out in any one or several of three ways:

- Internally, by a director, manager or employee, either individually or in collusion with others inside and/or outside the RFI conducting corporate service provider business;
- Externally, by a customer seeking to place, layer or integrate illicit assets; and
- Indirectly, by a third party service provider or by an RFI, independent professional or other intermediary facilitating transactions involving illicit assets on behalf of another person.

VI.28 The majority of this annex addresses attempted money laundering by customers. Money laundering risks involving third parties are addressed in paragraphs VI.112 through VI.116. Money laundering risks involving internal senior management, directors, managers or employees, are addressed via fit and proper requirements for corporate service providers and in paragraphs VI.34 through VI.37.

VI.29 Specific requirements for an RFI's detailed policies, procedures and controls are set forth in Chapters 2 through 11 of the main guidance notes.

VI.30 Detailed information is set forth in Chapter 1: Senior Management Responsibilities and Internal Controls.

<u>Links between corporate service provider business practices and AML/ATF policies, procedures and controls.</u>

VI.31 Persons carrying on corporate service provider business may be subject to Acts and Regulations that achieve some of Bermuda's AML/ATF objectives. These Acts and Regulations include, but are not limited to:

- Exchange Control Regulations 1973;
- Limited Partnership Act 1883;
- Exempted Partnerships Act 1992;
- Overseas Partnerships Act 1995;
- Corporate Service Provider Business Act 2012;

- Companies Act 1981; and
- Limited Liability Company Act 2016

VI.32 Persons carrying on corporate service provider business may also be subject to the requirements, principles, standards and procedures set forth in guidance documents. These guidance documents for corporate service providers include, but are not limited to:

- Statement of Principles 2014 made pursuant to section 6 of the Corporate Service Provider Business Act 2012;
- Code of Practice 2014 made pursuant to section 7 of the Corporate Service Provider Business Act 2012;
- Guidance Notes 2014; and
- Corporate Governance Policy 2016.

VI.33 The requirements of the Acts, Regulations and additional guidance documents described in paragraphs VI.31 through VI.32 provide a suitable foundation for the AML/ATF policies, procedures and controls that Bermuda RFIs are required to adopt and implement. An RFI should not presume, however, that its existing processes are sufficient. Each RFI must ensure that it meets each of its AML/ATF obligations under the Bermuda Acts, Regulations and these guidance notes, whether as part of its existing business processes or through separate processes.

Ownership, management and employee checks

VI.34 To guard against potential money laundering involving owners, directors, managers and employees of corporate service providers, RFIs conducting corporate service provider business should screen such persons against high standards in accordance with paragraphs 1.70 through 1.74.

VI.35 RFIs should ensure that screenings are conducted both for the RFI itself and for any intermediary or third party service provider.

VI.36 Where any screening is conducted by a third party, the RFI should have procedures to satisfy itself as to the effectiveness of the screening procedures the third party uses to ensure the competence and probity of each person subject to screening.

VI.37 Working with intermediaries and third party service providers that are licenced and that apply AML/ATF measures at least equivalent to those in Bermuda is likely to reduce the measures a Bermuda RFI conducting corporate service business will need to undertake in order to meet its screening obligations.

Risk-based approach for RFIs conducting corporate service provider business

VI.38 RFIs conducting corporate service provider business must employ a risk-based approach in determining:

- Appropriate levels of customer due diligence (CDD) measures;
- Proportionate risk-mitigation measures to prevent the abuse of the RFI's products, services and delivery channels for ML/FT purposes;
- The scope and frequency of on-going monitoring; and
- Measures for detecting and reporting suspicious activity.

VI.39 The purpose of an RFI applying a risk-based approach is to balance the cost of AML/ATF compliance resources with a realistic assessment of the risk of the RFI being used in connection with ML/TF. A risk-based approach focuses resources and efforts where they are needed and where they have the greatest impact in preventing and suppressing ML/TF.

VI.40 The higher the risk an RFI faces from any particular combination of customer, product, service, transaction, delivery channel or geographic connection, the stronger and/or more numerous the RFI's mitigation measures must be.

VI.41 Each RFI should ensure that it has sufficient capacity and expertise to manage the risks it faces. As risks and understandings of risk evolve, an RFI's capacity and expertise should also evolve proportionally.

VI.42 RFIs conducting corporate service provider business are gatekeepers who, in addition to serving the interests of their customers, serve the broader interests of the public. An RFI's assessments of the ML/TF risks associated with a customer or transaction should be conducted independently, and in a manner that demonstrates high standards of professionalism extending beyond simply fulfilling the requirements of the Acts and Regulations.

VI.43 Legal persons, including corporates vary greatly in terms of size, complexity, activities undertaken and the degree to which their control and ownership structures are transparent. Corporates listed on an appointed stock exchange tend to be larger, more complex and, due to their public ownership, more transparent. Privately held corporates may be of a range of sizes and complexity, but tend to be less transparent.

VI.44 Regardless of a particular legal entity features, RFIs must use a risk based approach to determine whether there are legitimate commercial purposes for the size, structure and level of transparency of each customer and whether the customer or business relationship entails a heightened level of ML/TF risk.

VI.45 Although RFIs conducting corporate service provider business should target compliance resources toward higher-risk situations, they must also continue to apply risk mitigation measures to any standard- and lower-risk situations, commensurate with the risks identified. The fact that a customer or transaction is assessed as being lower risk does not mean the customer or transaction is not involved in ML/TF.

VI.46 RFIs should document and be in a position to justify the basis on which they have assessed the level of risk associated with each particular combination of customer, product, service, transaction, delivery channel or geographic connection.

VI.47 When designing a new product or service, an RFI conducting corporate service provider business must assess the risk of the product or service being used for ML/TF.

VI.48 Detailed information on the requirement that RFIs use a risk-based approach to mitigate the risks of being used in connection with ML/TF is set forth in Chapter 2: Risk-Based Approach.

ML/TF risks in the provision of corporate services

VI.49 Using the risk-based approach, each RFI conducting corporate service provider business should determine the amount of ML/TF risk it will accept in pursuit of its business goals.

VI.50 Nothing in the Acts or Regulations prevents an RFI from deliberately choosing to accept higher-risk business. Each RFI must, however, ensure that it has the capacity and expertise to apply risk mitigation measures that are commensurate with the risks it faces, and that it does effectively apply those measures.

VI.51 Corporate services are used more frequently for the layering stage of money laundering than for the initial placement of criminally involved funds. Criminals seeking to launder money with the involvement of a corporate service provider business are attracted primarily by:

- Business structures that obscure the identity of the private individuals who own and control the entity;
- The possibility of legally relocating assets from one jurisdiction to another; and
- The use of corporate service providers (gatekeepers) as nominee directors and shareholders to hide the ownership and control of assets;

VI.52 The level of risk associated with corporate service provider business depends in part on the services the RFI provides. The level of risk is generally higher where:

- The RFI is involved in the management of a customer's financial affairs;

- A customer has a complex structure or legal arrangement;
- A customer has multiple accounts and/or is engaged in complicated transfers and transactions; or
- A customer's business involves legal entities formed or registered under foreign law such that the ownership and control structure of each entity is not readily understood.

VI.53 For example, the risks faced by an RFI acting as a company director involved in the management of a customer's financial affairs will be significantly higher than the risks faced by an RFI that merely administers the identification and appointment of directors who are not employed by the RFI.

VI.54 Where an RFI provides registered office or registered agent services, but does not have direct control over the customer legal entity, the RFI should consider obtaining legal advice on whether any action by the customer could be imputed to the RFI.

VI.55 Where an RFI supplies directors to a customer with a split board arrangement, the RFI should consider obtaining legal advice on the level of responsibility it could face due to the customer's actions.

VI.56 Where a customer requests any, mail holding arrangement, or care of ("c/o") mail arrangement, the RFI should obtain the reasons for and details of the arrangement, conduct enhanced monitoring and consider whether this deliberate request is meant to obscure who ultimately owns and controls the company. The RFI should consider what other action is required due to the higher risk of ML/TF, consider business termination and consider filing a suspicious activity report depending on the circumstances.

VI.57 Specific indicators of higher risk in corporate service provider business are discussed in detail in paragraphs I.187 through I.193 of this annex.

Customer due diligence

VI.58 RFIs conducting corporate service provider business must carry out customer due diligence (CDD).

VI.59 Detailed information on customer due diligence is set forth in chapters 3, 4, and 5 of the main guidance, and paragraphs VI.60 through VI.159 of this annex.

VI.60 Carrying out CDD allows RFIs to:

- Guard against impersonation and other fraud by being satisfied that customers are who they say they are;
- Know whether a customer is acting on behalf of another;

- Identify any legal barriers (e.g. international sanctions) to providing the product or service requested;
- Maintain a sound basis for identifying, limiting and controlling risk exposure;
- Avoid committing offences under POCA and ATFA relating to ML/TF; and
- Assist law enforcement by providing information on corporate service provider customers or activities being investigated.

VI.61 CDD measures that must be carried out include:

- Identifying and verifying the identity of each customer;
- Understanding the purpose and intended nature of the customer's business relationship with the RFI;
- Identifying the source of wealth and source of funds associated with the customer;
- Gathering information sufficient to understand the legal form, ownership structure and control structure of the customer under the domestic and/or foreign law governing the customer's formation, registration and operation;
- Identifying and verifying signatories, directors and other persons exercising control over the management of the customer or its relationship with the RFI;
- Identifying and taking reasonable measures to verify the identity of the beneficial owner(s) of the customer; and
- Updating the CDD information at appropriate times. This includes ensuring that information on the ultimate beneficial owners and/or controllers of customer companies, partnerships and other legal entities is known to the RFI, properly updated and recorded.

VI.62 Detailed information on CDD for legal persons and other legal arrangements is set forth in paragraphs 4.75 through 4.135.

Purpose and intended nature of the customer's business relationship with the RFI

VI.63 An RFI must understand the purpose and intended nature of each proposed business relationship or transaction. In some instances the purpose and intended nature of a proposed business relationship may appear self-evident. Nonetheless, an RFI must obtain information that enables it to document and categorise the nature, purpose, size and complexity of the business relationship, such that it can be effectively monitored.

VI.64 To obtain an understanding sufficient to monitor a corporate service provider business relationship or transaction, an RFI should collect information, including, but not limited to:

- The customer's goals for the corporate service provider business relationship or transaction;
- The source of wealth and source of funds to be used in the corporate service provider business relationship or transaction;

- The anticipated type, volume, value, frequency, duration and nature of the activity that is likely to be undertaken through the corporate service provider business relationship or transaction;
- The geographic connections of the customer and each beneficial owner, administrator, advisor, operator, employee, manager, director or other person who is able to exercise significant power over the corporate service provider business relationship or occasional transaction;
- The means of payment (cash, wire transfer, other means of payment);
- Whether there is any mail holding arrangement, or care of ("c/o") mail arrangement, and if so, the reasons for and details of the arrangement; and
- Whether any payments are to be made to or by third parties, and if so, the reasons for and details of the request.

Source of wealth and source of funds

VI.65 Enquiries regarding the source of wealth and source of funds are among the most useful sources of information leading to knowledge, suspicion or reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing.

VI.66 RFIs should make enquiries as to how a customer has acquired the wealth, whether in currency, securities or any other assets, to be used with regard to the corporate service provider business relationship or transaction.

VI.67 The extent of such enquiries should be made using a risk-based approach.

VI.68 RFIs should also ensure that they understand the source of funds and specific means of payment, including the details of any account that a customer proposes to use.

VI.69 Additional information on source of funds and source of wealth is set forth in paragraphs 5.110 through 5.113 of the main guidance.

Definition of customer in a corporate service provider business context

VI.70 An RFI's customer is generally a private individual, legal person, trust or other legal arrangement with and for whom a business relationship is established, or with or for whom an occasional transaction is carried out. A given corporate service provider business relationship or transaction may have more than one person who is a customer.

VI.71 A customer that is not a private individual generally involves a number of individuals, such as the directors, trustees, beneficial owners and other persons who directly or indirectly own or have the ability to control the customer. An

RFI's customer is not only the customer itself, but also the individuals who comprise the customer entity and its relationship with the RFI.

VI.72 For the purposes of these guidance notes, a customer includes each of the following:

- Each private individual, legal person, trust or other legal arrangement that is or comprises a **customer** seeking a corporate service provider business product or service; and
- Each **beneficial owner** of a customer.

VI.73 Where, for example, a company approaches a corporate service provider to identify a suitable director, and the director who is placed with the company pays the corporate service provider for assistance in securing the placement, then the company, its beneficial owners and the director identified by the corporate service provider are customers of the corporate service provider.

VI.74 Full information on the meaning of customer, business relationship and occasional transaction, and on identifying and verifying individuals, legal persons, trusts and other legal arrangements is set forth in Chapter 4: Standard Customer Due Diligence Measures.

Definition of beneficial owner in a corporate service provider business context

VI.75 Irrespective of the geographic location of a customer, the complexity of a customer's structure or the means by which any business relationship is initiated, RFIs must know the identity of the persons who effectively own and control a customer.

VI.76 Under Regulation 3(11), corporate service provider businesses must consider as beneficial owners any persons, whether private individuals, legal persons or legal arrangements, that effectively own or control more than 10% of a customer's funds, assets or voting rights, or, in the case of trusts or similar legal arrangements, any persons entitled to a specified interest in at least 10% of the capital of the trust property. The meaning of 'control' and 'own' in this context should be interpreted broadly to comprise the capacity to:

- Manage funds, assets, accounts or investments without requiring further authorisation;
- Direct management to take or refrain from taking an action;
- Override internal procedures and control mechanisms;
- Derive benefit, whether presently or in the future;
- Exercise a specified interest, whether presently or in the future; and/or
- Add or remove beneficiaries, trustees, signatories or other persons associated with a customer, partners, general partners or members.

VI.77 Where control or ownership is held by another legal person or legal arrangement, RFIs should consider as a beneficial owner each private individual who ultimately controls or owns that other legal person or legal arrangement.

VI.78 RFIs must consider as beneficial owners those persons who own or control a customer or its management, directly or indirectly, through any bearer or nominee arrangement.

VI.79 Information on the identification and verification of beneficial owners is set forth in Regulation 3 and Chapter 4: Standard Customer Due Diligence Measures.

VI.80 Additional information specific to the beneficial ownership of trusts is set forth in Regulation 3(3) and paragraphs I.78 through I.87. Information specific to control over a trust is set forth in Regulation 3(4) and paragraphs I.65 through I.70.

Obtaining and verifying customer identification information

VI.81 RFIs must obtain and verify identification information for each person who is a customer in the corporate service provider business context.

VI.82 A person who is a customer in the corporate service provider business context may be an individual, a legal person, a trust or other legal arrangement. For each type of customer, RFIs should follow the identification and verification requirements in Chapter 4: Standard Customer Due Diligence Measures, as supplemented by any relevant Annexes.

VI.83 In addition to the information required for all customers, RFIs must obtain the following identification information in relation to each corporate customer:

- Full name and any trade names;
- Date and place of incorporation, registration or establishment;
- Registered office address and, if different, mailing address;
- Address of principal place of business;
- Whether and where listed on an exchange;
- Official identification number (where applicable); and
- Name of regulator (where applicable).

VI.84 RFIs must verify the following in relation to each corporate customer:

- Full name;
- Date and place of incorporation, registration or establishment;
- Official identification number (where applicable); and
- Current existence of the corporate.

VI.85 Partnerships that are legal persons should be identified and verified using the guidance for legal persons set forth in paragraphs 4.75 through 4.96. In such

cases, for the purposes of verification, RFIs may obtain sight of and retain record of the following documents in lieu of or in addition to a certificate of incorporation, articles of association or equivalent constitutional documentation:

- Partnership agreement; and/or
- Registered business name certificate.

VI.86 Where a customer is an unincorporated partnership or business, the RFI must determine whether to treat as customers the persons owning and controlling the partnership or business, or whether to treat as a customer the underlying business.

VI.87 The RFI should verify the existence, ownership and control structure of a corporate by:

- Confirming the corporate's listing on an appointed stock exchange;
- Confirming that the corporate is listed in the company registry of its place of formation and has not been, and is not in the process of being, dissolved, struck off, wound up or terminated;
- Obtaining sight of and retaining record of the corporate's certificate of incorporation; and/or
- Obtaining sight of and retaining record of the corporate's memorandum and articles of association or equivalent constitutional documentation.

VI.88 Regardless of the method(s) used, all required information must be verified.

VI.89 Where an RFI is unable to complete verification using the methods contained in paragraph VI.87, where the size or complexity of a corporate is significant, where the ownership or control structure of a customer is unclear, or where a business relationship is otherwise assessed as higher risk, the RFI should consider the extent to which additional evidence is required. Additional means of verification may include:

- Reviewing an independently audited copy of the latest report and accounts;
- Reviewing a copy of the director or shareholder's register;
- Reviewing the board resolution authorising the transaction or business relationship and recording signatories;
- Reviewing the ownership and control structure of any group of which the customer is part;
- Engaging a business information service or a reputable and known firm of lawyers or accountants to confirm the documents submitted;
- Utilising independent electronic databases; and
- Personally visiting the principle place of business.

VI.90 Where the customer is an unincorporated partnership or business, RFIs must verify the following:

- Full name;
- Business address;
- Official identification number (where applicable);
- Current existence of the customer;
- Ownership and control structure of the customer;
- Subject to paragraphs VI.97 and VI.98, the identity of all partners, principals, members, directors and other persons exercising control over the management of the unincorporated partnership or business; and
- The identity of all other persons purporting to act on behalf of the customer or by whom binding obligation may be imposed on the customer.

VI.91 Full information on identifying and verifying partnership customers is set forth in Chapter 4: Standard Customer Due Diligence Measures.

VI.92 Full information on identifying and verifying trust customers is set forth in Chapter 4: Standard Customer Due Diligence Measures and in Annex I.

Obtaining and verifying beneficial owner information

VI.93 RFIs conducting corporate service provider business must obtain identification information, in line with the guidance for private persons, and, where relevant, legal persons, for the individuals who ultimately own and control any customer that is a legal person, trust or other legal arrangement, including, but not limited to:

- All directors, signatories and other persons exercising control over management of the corporate;
- All private individuals who, either directly or indirectly via one or more other individuals, legal persons or legal arrangements, ultimately control or own more than 10% of a customer's funds, shares, assets or voting rights or interest; and
- All other persons purporting to act on behalf of the corporate or by whom a binding obligation may be imposed on the corporate.

VI.94 A limited exception to this fundamental rule may apply where a corporate customer's securities are listed on an appointed stock exchange. Additional information on this exception is set forth in paragraphs 4.95 through 4.96 of the main guidance notes.

VI.95 RFIs must verify the following in relation to each corporate customer:

- The ownership and control structures of the corporate;
- Subject to paragraphs VI.97 and VI.98, the identity of all directors, signatories and other persons exercising control over management of the corporate; and
- The identity of all other persons purporting to act on behalf of the corporate or by whom binding obligations may be imposed on the corporate.

VI.96 In addition, and on the basis of an assessment of the ML/TF risks associated with a customer and its business relationship, RFIs conducting corporate service provider business must take reasonable measures to verify the identity of all private individuals who, either directly or indirectly via one or more other individuals, legal persons or legal arrangements, ultimately control or own at least 10% of a customer's funds, shares, assets or voting rights.

VI.97 Where the number of directors, partners, principals, members, signatories and other persons exercising control over management of the corporate is high, RFIs may use a risk-based approach to determine whose identity to verify. Where ML/TF risks are standard or low, RFIs should verify at least two of the relevant signatories and, where different, two directors or other individuals exercising significant control over management of the customer. The individuals verified should be those the RFI expects to hold signatory powers for the purpose of operating an account or exchanging instructions. Where the ML/TF risks are higher, or where a customer may be seeking to avoid the application of certain CDD measures, the RFI may find it necessary to verify all individuals who directly or indirectly own or control more than 10% of the shares, voting rights or interest in the customer, all directors and other individuals exercising significant control over the management of the customer.

VI.98 Where any individual associated with the customer is assessed as higher risk, for example, where a politically exposed person or a target of international sanctions is involved, or where a business relationship is assessed as higher risk for any reason, all signatories, directors and other individuals exercising control over management of the customer must be verified.

VI.99 An RFI conducting corporate service provider business should ensure that agreements with customers:

- Are maintained in writing;
- Include a clear description of the services to be provided, fees to be charged, and the manner in which fees are expected to be deducted or paid; and
- State how and by whom authorised requests for action are to be given.

VI.100 Where any customer has, or is requesting, a nominee service, the RFI should seek to identify the nominator and seek to understand why any beneficial owner does not wish to operate the customer entity in his or her own personal capacity.

VI.101 Where an RFI provides or arranges for others to provide a nominee service, the RFI should ensure that the written nominee agreement identifies the nominator and beneficial owners, and that the RFI retains a copy of the agreement in its records.

VI.102 Where a customer is an agent acting on behalf of a principal, the principal must also be subject to CDD, including identifying and verifying the principal as a customer, and identifying and taking reasonable measures to verify the persons who own and control the principal and its management.

VI.103 Full information on identifying and verifying partnership customers and the beneficial owners and persons exercising significant control over partnerships is set forth in paragraphs 4.122 through 4.135 of the main guidance notes.

VI.104 Full information on identifying and verifying trust beneficiaries is set forth in Chapter 4: Standard Customer Due Diligence Measures and in Annex I.

Timing of customer due diligence

VI.105 An RFI must apply CDD measures when it:

- Establishes a business relationship;
- Carries out an occasional transaction in an amount of $15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked, or carries out any wire transfer in an amount of $1,000 or more (see Chapter 8: Wire Transfers);
- Suspects money laundering or terrorist financing; or
- Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

VI.106 Where the product or service is a one-off transaction amounting to less than $15,000, for example, company formation but no further services are required that would involve an on-going business relationship with the client, then, in line with the RFI's risk assessment, verification of identity may not be necessary..

VI.107 However, where a customer who has carried out a one-off transaction amounting to less than $15,000 requests a future or on-going service, or returns to carry out further transactions, the RFI should consider that it is entering into a business relationship requiring customer due diligence measures.

VI.108 Without exception, RFIs conducting corporate service provider business should always identify the customer, the relevant persons comprising the customer, beneficial owners, persons exercising significant control, the purpose and intended nature of the business relationship, and the source of wealth and source of funds before the establishment of a business relationship or the carrying out of an occasional transaction. RFIs conducting corporate service provider business may not delay the exercise of CDD until during or after the establishment of a business relationship. See paragraph 3.17.

VI.109 Verification should take place:

- Before the RFI accepts a new customer;
- Before the RFI provides any service as part of a business relationship or occasional transaction;
- Before the RFI allows the exercise of any power or control;
- When a new party becomes entitled to exercise power or control; and
- Subsequently when there is any change in information previously provided, or when otherwise deemed necessary due to information obtained through risk assessment or on-going monitoring.

VI.110 Each time a new or existing customer adds assets to any customer portfolio managed or overseen by an RFI, the RFI should obtain and verify the source of the assets and the objectives of the customer.

VI.111 Detailed information on the timing of CDD measures is set forth in Chapter 3: Overview of Customer Due Diligence.

Previous due diligence and reliance on third parties

VI.112 Paragraphs 5.118 through 5.148 set forth the circumstances in which reliance on a third party is permissible. Paragraphs 3.22 through 3.24 provide additional relevant guidance. In any reliance situation, however, the relying RFI retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

VI.113 Before an RFI conducting corporate service business can rely on CDD conducted by a third party, the RFI must determine whether the third party carried out at least the standard level of customer verification.

VI.114 An RFI that is taking over from a previous corporate service provider or acting as an additional corporate service provider should obtain sight of and retain record of all original due diligence documentation.

VI.115 Where an RFI determines that the information it has received is adequate, and all other criteria for relying upon a third party have been met, the RFI may determine that it has satisfied its CDD obligations.

VI.116 Where, however, an RFI determines that relevant documentation is not available, or is inadequate, the RFI will need to seek additional documentation.

Refusing or terminating corporate service provider business

VI.117 If for any reason an RFI is unable to complete CDD measures in relation to a customer, Regulation 9 establishes that the RFI must:

- In the case of a proposed business relationship or transaction, not establish that business relationship and not carry out that occasional transaction with or on behalf of the customer;

- In the case of an existing business relationship, terminate that business relationship with the customer; and
- Consider whether the RFI is required to make a Suspicious Activity Report to the Financial Intelligence Agency (FIA), in accordance with its obligations under POCA 1997 and ATFA 2004.

VI.118 Where an RFI conducting corporate service provider business decides that a business relationship must be terminated due to an inability to complete CDD, the RFI must take appropriate steps to stop acting as the corporate service provider or, as appropriate, not proceed with any proposed act, service, transaction or representation. Where there are no grounds for filing a Suspicious Activity Report, any client funds should be returned to the client by bank transfer, wherever possible, into the customer's bank account from which the RFI originally received the funds.

VI.119 Where an RFI declines or terminates business that it knows is, or suspects might be, criminal in intent or origin, the RFI must refrain from referring such declined business to another person.

Customer transactions involving cash or bearer instruments

VI.120 In the context of corporate service provider business, RFIs should limit the acceptance or delivery of cash or other bearer negotiable stores of value to *de minimus* amounts. In extremely rare circumstances where this guidance is not followed, an RFI should be prepared to demonstrate that it has determined and applied appropriate risk-mitigation measures, and documented relevant policies, procedures and controls applicable to its business and the particular customer. Any cash or bearer instrument transaction that is not of a *de minimus* amount should be reported to the RFI's Reporting Officer.

VI.121 Paragraph 7.14 states that each RFI should establish norms for cash transactions and procedures for the identification of unusual cash transactions or proposed cash transactions.

VI.122 Paragraphs 4.97 through 4.101 provide additional guidance on the use of bearer instruments.

Applicability of simplified due diligence to corporate service provider business

VI.123 Simplified due diligence involves the application of reduced or simplified CDD measures in specified circumstances.

VI.124 RFIs may consider applying reduced or simplified due diligence measures only where the risk assessment process results in a finding of lower than standard risk.

VI.125 Where a corporate customer's securities are listed on an appointed stock exchange, the corporate is publicly owned and RFIs may forego verifying the identity of the corporate's beneficial owners, provided that:

- The corporate is listed on an appointed stock exchange that is subject to Bermuda disclosure obligations or to disclosure obligations equivalent to those in Bermuda; or
- The corporate is a majority-owned and consolidated subsidiary of such a listed company.

VI.126 Where a corporate is listed outside of Bermuda on a market that is not subject to disclosure obligations equivalent to those in Bermuda, RFIs must apply the verification requirements normally applicable to private and unlisted companies.

VI.127 Where a customer involves an entity for which simplified due diligence is appropriate, RFIs must nonetheless adhere to the guidance notes in identifying and verifying signatories and other persons connected with the customer.

VI.128 Detailed information on the applicability of simplified due diligence is set forth in paragraphs 3.17 and 5.1 through 5.14.

Enhanced due diligence for corporate service providers

VI.129 Enhanced due diligence is the application of additional CDD measures where necessary to ensure that the measures in place are commensurate with higher ML/TF risks.

VI.130 Regulation 11 requires RFIs to apply enhanced due diligence in all situations where a customer or the products, services, delivery channels, or geographic connections with which the customer engages present a higher than standard risk of money laundering or terrorist financing.

VI.131 In addition, enhanced due diligence must be applied in each of the following circumstances:

- The business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions (see paragraphs 5.19 through 5.20);
- The customer or beneficial owner has not been physically present for identification purposes (see paragraph 5.26 through 5.30); and
- The business relationship or occasional transaction involves a politically exposed person (see paragraphs 5.97 through 5.117).

VI.132 Where an RFI determines that enhanced due diligence measures are necessary, it must apply specific and adequate measures to compensate for the higher risk of money laundering.

VI.133 In selecting the appropriate additional measures to be applied, RFIs should consider obtaining additional information and approvals, including one or more of the following:

- Additional information on the customer, such as the persons that comprise, own and control the customer, the nature of the customer's business, volume of assets, and information available through public databases;
- Additional information on the nature and purpose of the business relationship (see paragraphs 4.1 through 4.4);
- Additional information on the source of wealth and source of funds of the customer (see paragraphs 5.110 through 5.113);
- Additional information on the reasons for planned or completed transactions; and
- Approval of the RFI's senior management to commence or continue the business relationship (see paragraph 5.109).

VI.134 In addition, RFIs should consider applying additional measures, such as:

- Updating more frequently the identification and verification data for the customer, its beneficial owner(s), and any other persons with who own or may exercise control over the customer;
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of controls applied and by identifying patterns of activity requiring further examination; and
- Requiring the first payment to be carried out through an account in the customer's name via an RFI subject to the Regulations, or via an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements;

VI.135 Detailed information on enhanced due diligence is set forth in Chapter 5: Non-Standard Customer Due Diligence Measures.

VI.136 Specific indicators of higher risk in corporate service provider business are discussed in greater detail in paragraphs VI.187 through VI.193 of this annex.

International sanctions

VI.137 RFIs conducting corporate service provider business should implement a sanctions compliance programme in line with the guidance set forth in Chapter 6: International Sanctions.

VI.138 RFIs should determine whether any persons connected with a customer, and the individuals behind any such persons that are legal entities, trusts or other legal arrangements, are sanctions targets.

VI.139 RFIs must be aware that, in contrast to AML/ATF measures, which permit corporate service providers some flexibility in setting their own timetables for verifying and updating CDD information, an RFI risks breaching a sanctions obligation as soon as a person, entity or good is listed under a sanctions regime in effect in Bermuda. In addition, whereas an RFI may choose to transact with a higher-risk individual or entity, it may not transact with any individual or entity subject to the Bermuda sanctions regime without first applying for and obtaining an appropriate licence.

On-going monitoring

VI.140 Regulations 7, 11(4)(c), 13(4), 16 and 18 require RFIs to conduct on-going monitoring of the business relationship with their customers.

VI.141 On-going monitoring in the context of corporate service business supports several objectives:

- Maintaining a proper understanding of a customer's owners, controllers and activities;
- Ensuring that CDD documents and other records are accurate and up-to-date;
- Providing accurate inputs for the RFI's on-going risk assessment processes;
- Testing the outcomes of the RFI's on-going risk assessment processes; and
- Detecting and scrutinising unusual or suspicious conduct in relation to a customer.

VI.142 RFIs conducting corporate service provider business should have adequate policies and procedures in place to confirm that they know on an on-going basis the current identity of each director, partner or officer and the current identity of all the persons who own and control the entities under administration.

VI.143 Failure to adequately monitor a customer's business relationship could expose an RFI to abuse by criminals and may call into question the adequacy of the RFI's AML/ATF policies, procedures and controls and the integrity or fitness and properness of the RFI's management.

VI.144 On-going monitoring of a business relationship includes:

- Scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of wealth and/or source of funds) to ensure that the transactions are consistent with the RFI's knowledge of the customer, the customer profile, and the persons who own and control the

customer;

- Investigating the background and purpose of all complex or unusually large transactions, and all unusual corporate structures and patterns of transactions which have no apparent economic or lawful purpose;
- Recording in writing the findings of investigations; and
- Reviewing existing documents, data and information to ensure that they are accurate, up-to-date, adequate, and relevant for the purpose of applying CDD measures in the context of corporate service provider business.

VI.145 Under the Limited Partnership Act 188,3 the Exempted Partnerships Act 1992 and the Limited Liability Company Act 2016, a corporate service provider, which maintains a register of members of an LLC, or a register of partners of a limited or exempted partnership, unless it holds an unlimited licence, may not register an issue or transfer of securities, unless the relevant authority has been notified. Any such issuance or transfer, will be effective only upon notice to the relevant authority as soon as practicable, but no later than 14 days after the change.

VI.146 RFIs conducting corporate service provider business therefore must ensure that information on the beneficial owners and/or controllers of customer companies, partnerships and other legal entities is known to the RFI and is properly recorded.

VI.147 RFIs conducting corporate service provider business should have policies, procedures and controls in place to monitor initial determinations of and subsequent changes to beneficial owner and controller information.

VI.148 Each RFI should ensure that its policies, procedures and controls dealing with the administration of shelf companies, bearer instruments and nominee arrangements are proportionate to the ML/TF risks involved.

VI.149 An RFI should require corporate customers to notify it of any material change to:

- Persons who are directors, signatories, beneficial owners or other persons exercising control over management of the corporate;
- Powers or authorities assigned to such persons; and
- Other changes to the control or ownership structures of the customer.

VI.150 It is the RFI's responsibility to maintain current information concerning the above.

VI.151 In addition, each time a customer makes a sizeable payment into a client money account, or otherwise contributes significant value to a business relationship or occasional transaction, an RFI should obtain and verify the source of the funds or value and the objectives of the customer.

VI.152 RFIs conducing corporate service provider business should ensure that where a customer transaction would normally be made using a customer account, but the

customer requests the transaction to be made using an RFI account, the reasons for this should be understood and evaluated to determine whether the conduct indicates higher ML/FT risk.

VI.153 On-going monitoring must be carried out on a risk-sensitive basis. Higher-risk customers and business relationships must be subjected to enhanced due diligence and more frequent and/or intensive on-going monitoring.

VI.154 Bearing in mind that some criminal activity may be so widespread as to appear to be the norm, RFIs should establish norms for lawful transactions and conduct in relation to corporate service provider customers, and the persons who own and control those customers. See paragraphs 7.11 through 7.14.

VI.155 Once an RFI has established norms for lawful transactions and conduct, it must monitor the business relationship, including transactions, patterns of transactions and conduct by customers and the persons who own and control those customers to identify transactions and conduct falling outside of the norm.

VI.156 The determination of norms for a category of customers or a category of persons who own and control a customer, should be based initially upon the information obtained in order to understand the purpose and intended nature of the customer and its business relationship with the RFI. See paragraph VI.64.

VI.157 Monitoring may take place both in real time and after the event, and it may be manual or automated. Irrespective, any system of monitoring should ensure at its core that:

- Customers, persons who own and control customers, transactions and conduct are flagged in exception reports for further examination;
- The exception reports are reviewed promptly by the appropriate person(s); and
- Appropriate and proportionate action is taken to reduce the possibility of money laundering or terrorist financing occurring without detection.

VI.158 Where an RFI accepts higher-risk business, it must ensure that it has the capacity and expertise to effectively conduct on-going monitoring of the customer, the persons who own and control the customer, and the business relationship with the RFI. See paragraph VI.50.

VI.159 Detailed information on on-going monitoring is set forth in Chapter 7: On-Going Monitoring.

Suspicious activity reporting

VI.160 The suspicious activity reporting requirements for RFIs are governed primarily by Sections 46 of POCA 1997, Sections 5 through 12 of ATFA 2004, and Regulations 16 and 17.

VI.161 RFIs conducting corporate service provider business must put in place appropriate policies and procedures to ensure that knowledge, suspicion, and reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing, are identified, enquired into, documented, and reported.

VI.162 The definitions of knowledge, suspicion, and reasonable grounds to know or suspect are set forth in paragraphs 9.6 through 9.10 of main guidance notes.

VI.163 Many customers will, for perfectly good reasons, have an erratic pattern of transactions or activity. A transaction or activity that is identified as unusual, therefore, should not be automatically considered suspicious, but should cause the RFI to conduct further, objective enquiries to determine whether or not the transaction or conduct is indeed suspicious.

VI.164 Enquiries into unusual transactions should be in the form of additional CDD measures to ensure an adequate, gap-free understanding of the relationship, including the purpose and nature of the transaction and/or conduct in question and the identity of the persons who initiate or benefit from the transaction and/or conduct.

VI.165 All employees, regardless of whether they have a compliance function, are obliged to report to the Reporting Officer within the RFI each instance in which they have knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

VI.166 An RFI's Reporting Officer must consider each report, in light of all available information, and determine whether it gives rise to knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

VI.167 Where, after evaluating an internal suspicious activity report, the Reporting Officer determines that there is knowledge, suspicion, or reasonable grounds to know or suspect that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing, the Reporting Officer must file an external suspicious activity report with the Financial Intelligence Agency.

VI.168 As of October 2011, the Financial Intelligence Agency no longer accepts any manually submitted suspicious activity reports (including those faxed or emailed). The Financial Intelligence Agency accepts only those suspicious activity reports that are submitted electronically via the go AML system, which is available at www.fia.bm.

VI.169 Where a Reporting Officer considers that an external report should be made urgently, initial notification to the Financial Intelligence Agency may be made by

telephone, but must be followed up by a full suspicious activity report as soon as is reasonably practicable.

VI.170 The Financial Intelligence Agency is located at 6th Floor, Strata 'G' Building, 30A Church Street, Hamilton HM11 and it can be contacted during office hours on telephone number (441)-292-3422, on fax number (441)-296-3422, or by email at info@fia.bm.

Failure to report and tipping-off offenses

VI.171 Where an employee fails to comply with the obligations under Section 46 of POCA 1997 or Schedule 1 of ATFA 2004 to make disclosures to a Reporting Officer and/or to the Financial Intelligence Agency as soon as is reasonably practicable after information giving rise to knowledge or suspicion comes to the attention of the employee, the employee is liable to criminal prosecution.

VI.172 The criminal sanction, under POCA 1997 and ATFA 2004, for failure to report, is a prison term of up to three years on summary conviction or ten years on conviction in indictment, a fine up to an unlimited amount, or both.

VI.173 Section 47 of POCA 1997 and Section 10 of ATFA 2004 contain tipping-off offences.

VI.174 It is a tipping-off offence under Section 47 of POCA 1997 and Section 10 of ATFA 2004 if a person knows or suspects that an internal or external report has been made to the Reporting Officer or to the Financial Intelligence Agency and the person discloses to any other person:

- Knowledge or suspicion that a report has been made; and/or
- Any information or other matter likely to prejudice any investigation that might be conducted following such a disclosure.

VI.175 It is also a tipping-off offence if a person knows or suspects that a police officer is acting, or proposing to act, in connection with an actual or proposed investigation of money laundering or terrorist financing and the person discloses to any other person any information or other matter likely to prejudice the actual or proposed investigation.

VI.176 Any approach to the customer or to an introducing intermediary should be made with due regard to the risk of committing a tipping-off offense. See paragraphs 9.83 through 9.84.

VI.177 Detailed information on suspicious activity reporting, including related offenses and constructive trusts is set forth in Chapter 9: Suspicious Activity Reporting.

Employee training and awareness

VI.178 The responsibilities of RFIs to ensure appropriate employee training and awareness are governed primarily by Regulations 16 and 18.

VI.179 RFIs must take appropriate measures to ensure that relevant employees:

- Are aware of the Acts and Regulations relating to ML/TF;
- Undergo training on how to identify transactions which may be related to ML/TF; and
- Know how to properly report suspicions regarding transactions that may be related to ML/TF.

VI.180 Each RFI must also ensure that relevant employees receive appropriate training on its AML/ATF policies and procedures relating to:

- Customer due diligence measures;
- On-going monitoring;
- Record-keeping;
- Internal controls; and
- Risk assessment and management.

VI.181 In a corporate service provider business context, training should enable employees to:

- Readily identify corporates, partnerships, trusts and other vehicles that may be structured for ML/TF purposes;
- Effectively vet customers and the persons who own and control them;
- Assess the risks associated with a customer; and
- Conduct on-going monitoring of the customer and its business relationship with the RFI.

VI.182 Where an employee exercises discretion for or in relation to a customer, the RFI must ensure that the employee has an appropriate level of knowledge and experience to exercise the discretion properly, in accordance with the duties and obligations arising under the Acts and Regulations. Training may supplement the requisite level of knowledge and experience, but likely cannot adequately replace it.

VI.183 Detailed information on employee training and awareness is set forth in Chapter 10: Employee Training and Awareness.

Record-keeping

VI.184 The record-keeping obligations of RFIs are governed primarily by Regulations 15 and 16.

As noted in VI. 146: RFIs conducting corporate service provider business must ensure that information on the ultimate beneficial owners and/or controllers of customer companies, partnerships and other legal entities is known to the RFI and is properly recorded. This information should be in a format that is easily accessible, up-to-date and available for inspection by the Bermuda Monetary Authority and other competent authorities.

VI.185 RFIs must keep specified records for a period of at least five years following the date on which the business relationship ends, or, in the case of an occasional transaction, following the date on which the transaction, or the last in a series of transactions, is completed.

VI.186 Detailed information on the records that must be kept is set forth in Chapter 11: Record-Keeping.

Risk factors for corporate service provider business

VI.187 In addition to the non-exhaustive list of risk factors set forth in paragraph 2.35, RFIs conducting corporate service provider business should consider sector-specific risk factors, including those in paragraphs VI.188 through VI.193 below, in order to fully assess the ML/TF risks associated with a particular business relationship. The non-exhaustive list of sector-specific risk factors addresses customers, products, services, transactions, delivery channels, third party service providers and geographic connections.

VI.188 Customer risk factors include, but are not limited to:

- The use of complex networks of legal arrangements where there is no apparent rationale for the complexity, or where the complexity appears to be intended to conceal the true ownership or control arrangements from the RFI;
- Any unexplained relationship between a customer, the persons acting on behalf of the customer, the persons owning and controlling the customer and any third parties;
- Unjustified delays in the production of identity documents, underlying company accounts or other requested information;
- Situations in which it is difficult to identify the individuals who own and control a customer. This includes situations where identification is hindered because the persons who appear to own or control a customer are legal persons, trusts or other types of legal persons;
- Frequent changes to shareholders, directors or other persons owning or controlling any underlying legal person, trust or other legal arrangement;
- The unnecessary or excessive use of nominee shareholders or directors;
- The unnecessary granting of a power of attorney;

- The use of opaque or complex legal persons or arrangements where the customer is not open about their purpose;
- The involvement of any politically exposed person (PEP) as a person owning, controlling or representing the customer, or as a person otherwise connected with the customer;
- The involvement of any third party or intermediary that would be subject to regulation in Bermuda, but is not subject to equivalent regulation in its jurisdiction;
- A client who is unwilling or unable to provide satisfactory information to verify the source of wealth or source of funds;
- Levels of assets or transactions that exceed what a reasonable person would expect of a customer with a similar profile; and
- A customer offering to pay extraordinary fees for unusual services, or for services that would not ordinarily warrant such a premium.

VI.189 Products and services risk factors include, but are not limited to:

- The unexplained and illogical use of corporate structures, legal arrangements, shelf companies, split boards, nominee shares or the use of bearer negotiable instruments;
- The unexplained and illogical use of mail hold or care of ("c/o") mail services;
- Any request that might indicate that the stated purpose of the customer's structure, or the stated purpose of the customer's business relationship with the RFI, is not the true purpose;
- Any request to manage a customer's finances or bank accounts where such a customer would ordinarily manage its own finances and banking;
- Requests for payment to be made via the RFI's client money account, where such a payment would normally be made from a customer's own account;
- Requests for use of a pre-constituted shell company in a jurisdiction that allows the company's use, but does not require ownership and control information to be updated;
- Requests to create a corporate structure, or carry out a transaction with undue complexity, or with no discernable commercial purpose;
- Requests to create a corporate structure, or to carry out a transaction, with undue speed, particularly where the person associated with the customer requests that any of the due diligence process be completed after the establishment of the entity, or after the initiation of a transaction; and
- Requests for anonymity. While a customer's requests for their business to be conducted discreetly should not automatically be inferred as illegitimate, requests for anonymity may be indicative of higher risk.

VI.190 Transaction risk factors include, but are not limited to:

- A customer that, once established, receives sizeable or multiple cash deposits, or deposits from multiple sources;

- Transactions involving gambling, money service businesses, or cash-intensive businesses, or the proceeds of such categories of business;
- Transactions involving prohibited items such as armaments,
- Large cash transactions in circumstances where such a transaction would normally be made by cheque, banker's draft or wire transfer;
- Transfers of funds without a clear connection to the actual activities of the customer entity;
- Transfers of funds that are not in line with the stated business activities of the customer;
- Customers requesting transfers to or from overseas locations with instructions for payment to be made in cash;
- Sizeable third party cheques endorsed in favour of the customer or a person associated with the customer;
- Large payments for unspecified services to consultants, employees or other parties;
- Purchase or sale transactions significantly above or below the market price;
- Commercial, private or real property transactions that have no apparent legitimate business, tax, legal or family governance purpose;
- Unusual, complex or uncharacteristically large transactions;
- Transactions of a size or volume that exceeds what a reasonable person would expect of a customer with a similar profile, or given the nature and stated purpose of the business relationship or transaction;
- Occasional transactions giving rise to suspicion; and
- Requests for funds, shares or other assets to be transferred to PEPs or higher-risk charities or other not-for-profit organisations not subject to effective supervision and monitoring.

VI.191 Delivery channel risk factors include, but are not limited to:

- Non face-to-face relationships with customers and the persons associated with them;
- Any request to carry out significant transactions using cash, or using any payment or value transfer method that obscures the identity of any of the parties to the transaction; and
- The use of a third-party intermediary, agent or broker, particularly where such a person would be subject to regulation in Bermuda, but is not subject to equivalent regulation in its jurisdiction.

VI.192 Third party risk factors include, but are not limited to:

- The involvement of any third party in carrying out any AML/ATF function in relation to a customer, including reliance upon, or outsourcing to, any third party that has not been sufficiently reviewed for compliance with paragraphs 5.118 through 5.178;

- Any unexplained relationship between a customer, the persons acting on behalf of the customer, the persons owning and controlling the customer and any third parties; and
- The use of a third-party intermediary, agent or broker, particularly where such a person would be subject to regulation in Bermuda, but is not subject to equivalent regulation in its jurisdiction.

VI.193 Geographic risk factors include, but are not limited to:

- A customer entity established with funds originating from foreign banks in high-risk jurisdictions;
- A customer, person acting on behalf of the customer, person owning or controlling the customer or any third party associated with the customer who is a resident in, or citizen of, a high-risk jurisdiction;
- A corporate service transaction to or from a high-risk jurisdiction;
- A non-face-to-face corporate service transaction initiated from a high-risk jurisdiction;
- A corporate service transaction linked to business in or through a high-risk jurisdiction;
- Corporate service provider business involving persons or transactions with a material connection to a jurisdiction, entity, person, or activity that is a target of an applicable international sanction;
- Requests for use of a pre-constituted shell company in a jurisdiction that allows the company's use, but does not require ownership and control information to be updated; and
- A corporate service business relationship or transaction for which an RFI's ability to conduct full CDD may be impeded by a jurisdiction's confidentiality, secrecy, privacy or data protection restrictions.