GUIDANCE NOTES

FOR THE PREVENTION & DETECTION OF

MONEY LAUNDERING, TERRORIST FINANCING, PROLIFERATION FINANCING AND SANCTIONS

FOR THE ACCOUNTING SECTOR

Issued by the

Barristers and Accountants AML/ATF Board

Updated: June 2026

TABLE OF CONTENTS

CHAPTER 1: OVERVIEW

1.1 Accountants are key professionals in the business and financial sector who often facilitate vital transactions that underpin Bermuda's economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. Increasingly over the past decade, criminals have responded to the anti-money laundering, anti-terrorism and anti-proliferation financing measures taken by the traditional financial institutions and have sought other means to convert their proceeds of crime, or to mix them with legitimate income before they enter the banking system, thus making those proceeds of criminal conduct harder to detect. Frequently, professional advisors such as lawyers and accountants who interface with the financial sector have been used in some jurisdictions as a conduit for criminal property to enter the financial system and as such Bermuda's accounting and legal fraternity should be on guard to ensure that it is not used in this manner.

1.2 In particular, criminals and money launderers will often try to exploit the services offered by firms, through the business of undertaking property and financial transactions, setting up corporate and trust structures and when acting as directors or trustees. Furthermore, client accounts can provide a money launderer with a valuable, anonymous, route into the banking system.

1.3 The inter-governmental agencies and international standard-setting bodies, such as the Financial Action Task Force ("FATF"), have recognized the access that professional advisors provide for their clients to financial services and products, and have extended the scope of the international standards and recommendations to includes and accountants often referred to as 'gatekeepers'. As a well-regulated jurisdiction operating within the international financial arena, Bermuda has adopted these international standards to guard against money laundering, terrorist and proliferation financing and has integrated the requirements into its legal and regulatory framework.

1.4 The continuing ability of Bermuda's finance industry to attract legitimate clients with funds and assets that are clean and untainted by criminality depends, in large part, upon the Island's reputation as a sound, well-regulated jurisdiction. Therefore, any professional accountancy firm in Bermuda that is found to be involved in a money laundering, terrorist or proliferation financing scheme with knowledge or suspicion or reasonable grounds for suspicion of the connection to crime may face a range of penalties including the loss of its reputation, disciplinary action by the Institute of Chartered Accountants of Bermuda.

Every accountancy firm in Bermuda must recognize the role that it must play in protecting itself and its employees from involvement in money laundering, terrorist and proliferation financing, and in protecting the Island's reputation. This principle relates not only to business operations within Bermuda, but also operations conducted by Bermuda firms outside the Island.

1.5 These guidance notes (“Guidance Notes” or “Guidance”) are issued by the Barristers and Accountants AML/ATF Board (the "Board") for the purpose of providing guidance to

firms subject to its supervisory authority in relation to their obligations under Bermuda's legislative framework for the prevention and detection of money laundering, terrorist financing proliferation financing, and for compliance with sanctions measures.

These Guidance Notes are intended to provide general information and support understanding of the subject matter; however, they are not a substitute for applicable legislation or legal requirements. Users should refer directly to the relevant laws and regulations in force within their jurisdiction, as these take precedence over any guidance provided. In cases of uncertainty or conflict, the official legislative texts and, where appropriate, professional legal advice should be relied upon to ensure full compliance.

Firms are required to establish, implement and maintain effective systems, controls, policies and procedures to ensure compliance with the Proceeds of Crime Act 1997 ("POCA"), the Anti-Terrorism (Financial and Other Measures) Act 2004, the Proliferation Financing (Prohibition) Act 2017 ("ATFA"), Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (the "Regulations") (incorporating Proliferation Financing)[1] CPAB sanctions legislation, including the International Sanctions Act 2003 and related Regulations and any other CPBA enactment (together, the "Relevant Legislation").

Furthermore, these Guidance Notes are not intended to be exhaustive or a replacement for a firm's internal policies and procedures manual. However, section 30I(6) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (the "Supervision and Enforcement Act") provides that in deciding whether a regulated professional firm has failed to comply with a requirement of the Regulations, the designated professional body must consider whether the firm followed any relevant guidance which was at the time issued by the designated professional body. The Board is directed by section 5 of the Supervision and Enforcement Act to take measures necessary for the purpose of securing compliance by accountants with the Regulations. In the execution of this direction, the Board has wide powers under Part 4A of the Supervision and Enforcement Act, including powers of investigation, inspection, issuing mandatory directives, imposing civil penalties and publicizing any decision to impose a penalty on an accountant. It follows from the remit of the Board and the powers granted to it, together with the criminal provisions of section 33 of the Supervision and Enforcement Act and Regulation 19.

1.6 Bermuda conducted its latest National Risk Assessment in 2024. The accounting sector's inherent money laundering risk rating remained medium-low compared to previous risk assessments, reflecting a low level of money laundering threat alongside a medium level of inherent vulnerability. The sector's inherent terrorist financing risk was assessed as low, consistent with both low threat and vulnerability ratings. These assessments consider the sector's relatively small size, predominantly domestic client base, the nature of services provided, and a lower incidence of international transactions.

[1] Bermuda Anti-Money Laundering/Anti-Terrorist Financing/Counter – Proliferation Financing Policy; NAMLC 2025 – proposed legislation to be approved and passed by Parliament in 2026.

With respect to services risk, only a small number of firms were identified as providing limited services or engaging in transactions related to specified activities, the majority of which were associated with liquidations in their capacity as court-appointed liquidators. More broadly, firms that do engage in prescribed services tend to do so in the capacity of corporate service providers or trust companies, activities which fall outside the classification of accounting services.

Notwithstanding this, certain inherent vulnerabilities were identified, including exposure to foreign politically exposed persons, high-net-worth individuals, and non-resident clients, particularly those from higher-risk jurisdictions, as well as clients that are legal persons with complex ownership or control structures.

1.7 In implementing their AML/ATF/CPF obligations, firms should have regard to both the findings of the National Risk Assessment and the outcomes of their own business risk assessments. This combined approach helps ensure that identified risks are appropriately understood, assessed, and effectively mitigated through proportionate controls and measures.

CHAPTER 2: LEGISLATIVE and REGULATORY FRAMEWORK

2.1 Bermuda's key legislative enactments relevant to the accounting sector and pertaining to anti-money laundering, terrorist and proliferation financing primarily consists of the following (the "AML/ATF/CPF legislation"):

Statutes and Orders

- Revenue Act 1898
- Criminal Code Act 1907
- Taxes Management Act 1976
- Criminal Justice (International Cooperation) (Bermuda) Act 1994
- Proceeds of Crime Act 1997
- Proceeds of Crime (Designated Countries and Territories) Order 1998
- The Extradition (Overseas Territories) Order 2002
- International Sanctions Act 2003
- Anti-Terrorism (Financial and Other Measures) Act 2004
- Financial Intelligence Agency Act 2007 ("FIA Act")
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008
- Proceeds of Crime Appeal Tribunal Regulations 2009
- The Terrorist Asset-Freezing etc. Act 2010, (Overseas Territories) Order 2011, (An unofficial consolidation of the Terrorist Asset-Freezing etc. Act 2010)
- International Sanctions Regulations 2013
- Proliferation Financing (Prohibition) Act 2017
- Digital Asset Business Act 2018
- Beneficial Ownership Act 2025
- Proceeds of Crime (Miscellaneous) Act 2025
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Amendment Regulations 2026

Guidance Notes

- Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF
- Bermuda Financial Sanctions General Guidance for Financial Sanctions 2021
- BMA General Guidance Notes on AML/ATF (2024)
- FSIU Bermuda CPF Guidance (May 2025)

• NAMLC Counter-Proliferation Financing Policy (2025)

Supervisory Role

2.2 Regulation 2(1) defines a relevant person as a person to whom those Regulations apply, namely AML/ATF/CPF regulated financial institutions and independent professionals acting during business carried on by them in or from Bermuda. Accounting firms that are "relevant persons" pursuant to Regulation 2(1) must put in place risk-based systems and controls to guard against money laundering, terrorist and proliferation financing in accordance with Bermuda's requirements, which are based on the international standards as set by the FATF.

The FATF standards require all relevant persons must be supervised by an appropriate anti-money laundering supervisory authority. The Board has been established pursuant to section 8A of the Chartered Professional Accountants of Bermuda Act 1973 (the "CPAB Act"). The Minister of Justice by Order has designated the Board under section 4(1) of the Supervision and Enforcement Act as a supervisory authority for the purposes of section 3(1) (b) of that Act as the professional body for the relevant persons regulated by it. The Board's duties and powers are set out more particularly in sections 30C to 30N of the Supervision and Enforcement Act.

Guidance Notes

2.3 The Board's duties are set out in section 5 of the Supervision and Enforcement Act. Generally, section 5 directs the Board to effectively monitor the relevant persons for whom it is the supervisory authority and take necessary measures for the purpose of securing compliance by such persons with the Regulations. section 5(2) of that act states that a supervisory authority must issue from time-to-time guidance as to compliance with:

i. the Regulations;

ii. Part V of POCA;

iii. paragraph 1 of Schedule 1 to the ATFA;

iv. directions; and

v. international sanctions.

2.4 These Guidance Notes are being issued in accordance with section 5(2) of the Supervision and Enforcement Act. As "independent professionals" accountants are required by Regulation 4(b) to comply with those regulations and this Guidance when carrying out the services listed in Regulation 2(1). The objectives of these Guidance Notes are as follows:

- to outline the requirements of the AML/ATF/CPF legislation which applies to all professional accountants as defined by Regulation 2(1);
- to outline good practice for implementing the legal requirements;
- to set out the Board's requirements for professional accountants undertaking business providing accountancy services to other persons when participating in financial or real property transactions as set out in Regulation 2(1);

- to outline good practice in developing risk-based policies, procedures and risk mitigation mechanisms to prevent accountants from being used to facilitate money laundering, corruption, terrorist and proliferation financing, or the evasion of international sanctions[2];
- to provide a base from which individual accounting firms can design, document and implement policies, systems and controls and tailor their own policies and procedures for the prevention and detection of money laundering, terrorist and proliferation financing on a risk-weighted basis;
- to ensure that Bermuda matches international standards to prevent and detect money laundering, terrorist and proliferation financing;
- to provide direction on applying the risk-based approach effectively;
- to provide practical guidance on client due diligence, including identification and verification of identity;
- to provide practical guidance on the introduction and implementation of an annual audit to provide and document an independent and objective evaluation of the accountant's AML/ATF/CPF framework, and the reliability, integrity and completeness of the design and effectiveness of that accountant's AML/ATF/CPF risk management function, internal controls framework, and compliance; and
- to provide an information resource to be used in training and raising awareness of money laundering, terrorist and proliferation financing.

2.5 Where any affiliated company of an accounting firm is an AML/ATF/CPF regulated financial institution operating in or from within Bermuda as defined by Regulation 2(1) (which include Corporate Service Providers (CSP)) reference should be made to the Guidance Notes for AML/ATF/CPF regulated financial institutions issued by the Bermuda Monetary Authority (the "BMA") when considering their policies and procedures for the prevention of and detection of money laundering, terrorist and proliferation financing.

2.6 This Guidance is intended for use by senior management and compliance staff of a firm to assist in the development of systems and controls, and detailed policies and procedures. These Guidance Notes are not intended as an internal procedures manual or to provide an exhaustive list of systems and controls to counter money laundering, terrorist and proliferation financing. In applying the Guidance Notes, a firm should adopt an appropriate risk-based approach and should always consider what additional measures might be necessary to prevent its exploitation, and that of its services, by persons seeking either to launder money, engage in corrupt practices, finance terrorism or breach international sanctions.

Application of the Regulations

2.7 The Regulations apply to independent professionals pursuant to Regulation 4. An independent professional is defined in Regulation 2(1) as a professional legal advisor or

[2] Regulation 11(1)(ab)

accountant being a firm or sole practitioner in independent practice who by way of business provides legal or accountancy services to other persons when participating in financial or real property transactions concerning:

i. buying and selling of real property;

ii. managing of client monies, securities or other assets;

iii. management of bank, savings or securities accounts;

iv. organization of contributions for the creation, operation or management of companies; or

v. creation, operation or management of legal persons or arrangements, and buying and selling business entities.[3]

2.8 A person is defined as participating in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

2.9 Accountants providing services privately, on an unremunerated voluntary basis, are not covered by these Guidance Notes as they are not providing services 'by way of business'. Accountants involved in the provision of management consultancy or interim management should be alert to the possibility that they could fall within the scope of POCA, and by extension these Guidance Notes, to the extent they supply any of the specified services when acting under a contract for services during business.

Tax advisers

2.10 For the purpose of these Guidance Notes, those in business offering tax services are referred to as "tax advisers". Tax advisors are only required to implement the preventive measures outlined in these guidance notes when they engage in specified activities. The simple provision of tax advice without providing assistance in conducting transactions is not subject to AML/ATF/CPF requirements. Whilst tax advisers are more likely to identify offences relating to the avoidance or detection of tax offences, they need to be aware of the potential requirement to report knowledge or suspicion of proceeds derived from any serious crime which is encountered in the course of business as a tax adviser.

Audit services

2.11 Accountants are not subject to AML/ATF/CPF requirements when providing audit services. Auditors, nevertheless, need to take the possibility of money laundering, terrorist financing and proliferation financing into account in the course of carrying out procedures relating to fraud and compliance with the money laundering legislation. An auditor's wide access to documents and systems, and the need to understand the business, can make him ideally suited to identify possible suspicions of ML/TF/PF.

[3] Per POCA section 49(5)

Such higher-risk situations may include, but are not limited to, clients with complex or opaque ownership structures (including the use of multiple layers of legal persons or arrangements), transactions involving jurisdictions with weak AML/ATF/CPF controls or those subject to sanctions, unusually large or complex transactions that lack a clear economic or lawful purpose, significant use of cash or cash equivalents, frequent changes in ownership or control, and situations where there is reluctance or delay in providing requested information or documentation. Additional risk may arise where the client operates in sectors known to be vulnerable to financial crime, or where there are inconsistencies between the client's business activities and its financial profile. In such circumstances, auditors should apply heightened professional scepticism and consider whether enhanced due diligence or reporting to the Financial Intelligence Agency (FIA) is appropriate.

Audits of relevant persons as defined by POCA

2.12 In addition to reporting on their financial statements, auditors of such relevant persons as defined by POCA (e.g. financial institutions, real estate agents and brokers, casinos, high value dealers and independent professionals) should report to the Board on matters of significance that come to their attention in the course of their work. This includes non-compliance with legislation, departures from its requirements and suspicions that the directors and management of such entities are implicated in money laundering. Therefore, auditors of such businesses should not only be aware of the key provisions contained in the Regulations as they affect auditors themselves, but also the requirements of the relevant Regulations covering the business that they are auditing.

Insolvency practitioners

2.13 For the purpose of these Guidance Notes, those in the business of undertaking insolvency services are referred to as 'insolvency practitioners. In respect of advising clients on insolvency matters relating to individuals or entities, the requirements of the Regulations apply.

Engaging in specified financial activities

2.14 Accountants may also provide other services that could bring them within the scope of specified financial activities. Pursuant to section 42A(I) (Schedule 3) of POCA which may include;

i. undertaking investment related activity, including acting as a financial intermediary;

ii. advising on the setting up of trusts, companies or other bodies;

iii. acting as trustee, nominee or company director;

iv. giving advice on capital structures, acquisitions and securities issues;

v. providing safe custody services; and

vi. arranging loans.

2.15 Consequently, some accountancy firms are authorized and regulated by the BMA. Firms who are so regulated should refer to the separate guidance notes[4] issued by the BMA for AML/ATF/CPF Regulated Financial Institutions when drawing up their policies and procedures for the prevention and detection of money laundering, terrorist and proliferation financing in respect of those regulated activities.

2.16 The Board has confirmed that the following would not generally be regarded as falling within the services described in the definition of specified activities in Regulation 2(1):

i. payment on account of costs to accountancy professionals or payment of an accountant's bill;

ii. in respect of payments on account of costs, accounting firms should ensure that the payment is proportionate to the issue in respect of which the firm is asked to advise; and

iii. in respect of payment of an accountants' bill, if the accountant knowing that any property is or in whole or in part directly represents the proceeds of criminal conduct or suspects that the payment is made from the proceeds of criminal conduct, this would constitute an offence under section 45 of POCA.

Provision of accountancy advice

2.17 In relation to the provision of accountancy advice, an accountant needs to consider whether they are providing accounting advice or whether they are an accountant participating in a transaction by assisting in its planning or its execution. Ultimately, each case will have to be decided on its own facts, and it is a matter for each firm to form a view.

2.18 However, generally the giving of generic advice, or advice specific to a transaction in terms of whether such a transaction is possible under Bermuda Law or what factors are taken into account in making such a transaction possible, will only constitute the giving of accounting advice where the decision has not already been taken to proceed with the transaction.

2.19 Where a decision is made to proceed with a transaction set out in Regulation 2(1), drafting documentation to enable that transaction to proceed, or seeking information to advise further on the planning or execution of the transaction will fall within the scope of the Regulations.

Participation in litigation or a form of alternative dispute resolution.

2.20 In relation to litigation involving trusts where the proposed resolution includes a change in trusteeship or the application related to asking the Court to approve a future transaction, then the requirements of the Regulations may apply.

[4] Bermuda Monetary Authority, Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF August 2022

Penalties for Non-compliance

2.21 The Board has numerous powers to enforce compliance with the Regulations pursuant to Part 4A of the Supervision and Enforcement Act, including powers to require general or specific information, powers of entry to premises and physical inspection of an accountant's business, the issuing of directives e.g. to cease trading, and the imposition of civil penalties. In certain cases, it is a criminal offence to fail to comply.

2.22 In determining whether to impose a penalty on a firm that has failed to comply with the requirements of the Regulations, the Board must consider whether the firm followed any relevant guidance which was issued at the time by the designated professional body. The sanctions for failing to comply with the Regulations may include civil penalties up to $250,000.00 and publication of the decision to impose the penalty pursuant to sections 30I(1) and 30K of the Supervision and Enforcement Act.

2.23 Similarly, in determining whether a person has committed certain offences under POCA, for example section 46(2) of POCA (the offence of failing to disclose knowledge or suspicion or that they have reasonable grounds for suspicion of money laundering), the Supreme Court is required to take account of the guidance provided herein.[5] The sanctions for failing to comply with section 46(2) may be an unlimited fine or up to ten years imprisonment, or both. The sanction for failing to comply with section 9(3) of the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA) (the offence of failing to disclose information) may be a fine or imprisonment, or both.

2.24 Proliferation Financing - The Proceeds of Crime (Miscellaneous) Act 2025 was enacted in October 2025, amending section 49(1) of POCA to require that the National Risk Assessment framework now extends to proliferation financing risks. Further amendments to the Regulations integrate PF obligations throughout the regulatory framework for all AML/ATF/CPF Regulated Entities, including accountants. Regulated Professional Firms (RPFs) are required to identify, assess, and mitigate PF risks within their existing AML/ATF/CPF compliance programmes without the need to create separate processes. Chapter 12 provides additional details on this requirement.

2.25 These Guidance Notes are intended to provide general information and support understanding of the subject matter; however, they are not a substitute for applicable legislation or legal requirements. Users should refer directly to the relevant laws and regulations in force within their jurisdiction, as these take precedence over any guidance provided. In cases of uncertainty or conflict, the official legislative texts and, where appropriate, professional legal advice should be relied upon to ensure full compliance.

Furthermore, compliance with these Guidance Notes is not of itself a defense to offences under the money laundering legislation. However, courts will generally have regard to regulatory guidance when considering the standards of a professional person's conduct and whether they acted reasonably, honestly, and appropriately, and took all reasonable steps and exercised necessary due diligence to avoid committing the offence.

[5] Section 49M POCA

2.26 The consequences of non-compliance with the AML/ATF/CPF regulatory regime could include an inspection by the Board and the imposition of regulatory sanctions by the Board and CPAB.

CHAPTER 3: INTERNAL SYSTEMS AND CONTROLS

Regulation 16

3.1 Corporate governance is the system by which businesses are directed and controlled and the business risks managed. For accountants, money laundering, terrorist and proliferation financing are risks that must be managed in the same way as other business risks. These Guidance Notes describe the requirements for an accounting firm's general framework of systems and controls to manage the risk of money laundering, terrorist and proliferation financing and refers to the way in which those systems and controls are to be implemented into the day-to-day operation of the firm's business as policies and procedures.

3.2 Although the Board recognizes that legislation applies specifically to the relevant business activities of firms as outlined in Regulation 2(1), the AML/ATF/CPF legislation and the general offences and penalties cover all persons and all business activities within Bermuda.

3.3 For firms that do not engage extensively in regulated activities (as defined in Regulation 2(1)), it is advisable to evaluate money laundering, terrorist and proliferation financing risks on a case-by-case basis considering each client and engagement individually. When necessary, these firms should implement risk-based systems and controls. For more detailed guidance, refer to section 4 on the Risk Based Approach.

3.4 In accordance with Regulation 16(1) a relevant person must establish and maintain appropriate and risk sensitive policies and procedures relating to;

- client due diligence measures and ongoing monitoring;
- reporting;
- recordkeeping;
- internal control;
- risk assessment and management;
- the monitoring and management of compliance with and the internal communication of such policies and procedures to prevent activities related to money laundering, terrorist and proliferation financing.

In particular, where a firm intends to introduce a new product, practice or technology the firm must perform and document risk assessments prior to the launch of a new product, practice or technology[6].

3.5 An accounting firm must establish and maintain systems and controls to prevent and detect money laundering, terrorist and proliferation financing, that enable the business to:

i. apply appropriate client due diligence ("CDD") policies and procedures that consider vulnerabilities and risk which should include:

[6] Regulation 16 (1A)

a) the development of clear client acceptance policies and procedures;

b) identifying and verifying the identity of the client;

ii. monitor and review instances where exemptions are granted to policies and procedures, or where controls are overridden;

iii. report to the FIA when it has knowledge or suspicion or reasonable grounds for suspicion another person is involved in money laundering, terrorist and proliferation financing, including attempted transactions;

iv. ensure that relevant employees are adequately screened when they are initially employed, aware of the risks of becoming concerned in arrangements involving criminal money and terrorist financing, aware of their personal obligations and internal policies and procedures concerning measures to combat money laundering, terrorist and proliferation financing, and provided with appropriate training;

v. keep records in accordance with the Regulations;

vi. monitor compliance by overseas branches and subsidiaries with policies and procedures.

vii. screen against applicable sanctions lists maintained by HM Treasury (the UK Consolidated List) and report any matches to the Financial Sanctions Implementation Unit (FSIU); and

viii. assess and mitigate proliferation financing risks in accordance with the CPF requirements.

3.6 A firm must have policies and procedures in place to address any specific risks associated with client relationships established where the client is not physically present for identification purposes (i.e. non-face to face).

3.7 A firm must ensure that the systems and controls are implemented and operating effectively. For systems and controls (including policies and procedures) to be effective, they will need to be both appropriate to the size and business of the firm and aligned with the risk profile of the firm. In addition, the firm would need to take appropriate measures to guard against the use of technological developments in money laundering, terrorist or proliferation financing schemes. In particular, there should be policies and procedures in place to address specific risks associated with non-face to face business relationships or transactions, which should be applied when conducting due diligence procedures.

3.8. Issues which may be covered in an internal controls system include:

i. the level of personnel permitted to exercise discretion on the risk-based application of regulations, and under what circumstances;

ii. CDD requirements to be met for simplified, standard and enhanced due diligence;

iii. when outsourcing of CDD obligations or reliance on third parties will be permitted, and on what conditions;

iv. how the firm will restrict work being conducted on a file where CDD has not been completed;

v. the circumstances in which delayed CDD is permitted;

vi. when cash payments will be accepted;

vii. when payments will be accepted from or made to third parties; viii. the manner in which disclosures are to be made to the Reporting Officer.

3.9 Firms must integrate counter-proliferation financing controls into their existing AML/ATF systems and controls without the need to create separate processes. In accordance with FATF Criterion 1.15, firms must: (a) identify and assess PF risks; (b) document PF risk assessments and keep them current; (c) provide PF risk assessment information to relevant competent authorities on request; (d) have policies, controls and procedures approved by senior management to enable them to manage and mitigate PF risks that have been identified; (e) monitor the implementation of those controls and enhance them if necessary; and (f) take enhanced measures to manage and mitigate PF risks where higher risks are identified.

3.10 The firm may demonstrate that it has considered the effectiveness of the firm's risk management systems and controls where it, for example:

i. receives regular and timely information relevant to the management of the firm's money laundering, terrorist and proliferation financing risks;

ii. considers the adequacy of the management of the firm's money laundering, terrorist and proliferation financing risks;

iii. monitors the ongoing competence and effectiveness of the Compliance Officer and the Reporting Officer;

iv. considers the adequacy of resources to ensure effective compliance with the AML/ATF/CPF legislation and by extension this Guidance;

v. periodically reviews the adequacy of policies and procedures for higher risk clients;

vi. considers the adequacy of policies and procedures in place where CDD information and documentation is held by third parties such as group entities, outsourcing service providers, introducers and intermediaries;

vii. considers whether the incidence of suspicious activity reports (SARs) (or absence of such reports) has highlighted any deficiencies in the firm's CDD, monitoring or internal or external SAR policies and procedures, and whether changes are required to address any such deficiencies;

viii. takes into account changes made or proposed in respect of new legislation, regulatory requirements or guidance, or as a result of changes in business activities; and

ix. considers whether inquiries have been made by the FIA, or production orders received from the Bermuda Police Service, without issues having previously being identified by CDD or reporting policies and procedures.

3.11 The implementation of systems and controls for the prevention and detection of money laundering, terrorist and proliferation financing does not obviate the need for a firm to address cultural barriers that can prevent effective control. Human factors, such as the interrelationships between different employees within a firm, and between employees and clients, can result in the creation of damaging barriers.

3.12 Unlike systems and controls, the prevailing culture of an organization is intangible. As a result, its impact on the firm can sometimes be difficult to measure. The risk that cultural barriers might prevent the operation of effective systems and controls to prevent and detect money laundering, terrorist and proliferation may be minimized by senior management considering the prevalence of the following factors:

i. an assumption on the part of more junior employees that their concerns or suspicions are of no consequence;

ii. negative handling by partners or fee earners of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions;

iii. an unwillingness on the part of fee earners or other employees to subject high value (and therefore important) clients to effective CDD checks;

iv. pressure applied by senior management or fee earners outside Bermuda upon employees in Bermuda to conduct transactions without first obtaining all relevant CDD;

v. excessive pressure applied on fee earners to meet aggressive revenue-based targets, or where employee or fee earner remuneration or bonus schemes are exclusively linked to revenue-based targets;

vi. the familiarity of fee earners or other employees with certain clients resulting in unusual, complex, or higher risk activity and transactions within such relationships not being identified as such;

vii. the inability of employees to understand the commercial rationale for client relationships, resulting in a failure to identify non-commercial enterprises and therefore potential money laundering, terrorist and proliferation financing activity;

viii. a tendency for management to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily;

ix. an excessive desire on the part of employees to provide a confidential and efficient client service; and

x. non-attendance of partners or other members of management at anti-money laundering, terrorist and proliferation financing training sessions based on mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

Compliance Officer

3.13 Firms must designate a person employed at managerial level to serve as its Compliance Officer. In addition, the appointed Compliance Officer should not serve on the Board of Directors to ensure all conflicts of interest are mitigated. Firms shall be responsible for ensuring the Compliance Officer is adequately trained to carry out the role of Compliance Officer. The Compliance Officer must ensure that the necessary compliance program procedures and controls described above and throughout these Guidance Notes and as required by the Regulations are in place and coordinate and monitor the compliance program to ensure continuous compliance with the Regulations. Ideally the Compliance Officer should be resident in Bermuda. A Compliance Officer may also be appointed as a Reporting Officer. In the event that the Compliance Office is also appointed Reporting Officer, the Compliance Officer MUST be based in Bermuda in order that they may concurrently carry out their duty as Reporting Officer.

3.14 The Compliance officer must:

i. ensure that the necessary compliance program procedures and controls required by the Regulations are in place; and

ii. coordinate and monitor the compliance program to ensure continuous compliance with the Regulations.

3.15 Furthermore, firms must establish certain work conditions for the firm's Compliance Officer to meet their obligations such as providing:

- unrestricted access to all data, information and documentation necessary for the purposes of money laundering, terrorist and proliferation financing prevention and detection;
- adequate authorizations for an efficient conduct of tasks;
- adequate human resource, material and other work conditions;
- adequate premises and technical conditions guaranteeing a proper degree of data confidentiality and information protection available to the compliance officer;
- adequate IT support enabling on-going and safe monitoring field the activities in respect of money laundering, terrorist and proliferation financing prevention and detection;
- regular professional training in relation to money laundering, terrorist and proliferation financing prevention and detection; and
- replacement of the Compliance Officer during their absence.

3.16 Firms may outsource their systems and controls and processing to other jurisdictions or to other companies outside Bermuda within their group of companies. If the firm chooses to outsource its control functions, the third party must be regulated for AML/ATF/CPF purposes. However, an accounting firm cannot contract out of their legal obligations and as such they remain responsible for the systems and controls which have been outsourced and as such must actively manage the risk to the firm that this activity represents.

3.17 Group Policy and Domestic AML/ATF/CPF compliance obligations.

Where the firm operates as part of, or is affiliated with, a wider corporate group, it acknowledges that group-wide AML/ATF/CPF policies and procedures may be in place. The firm is required to additionally maintain an independent domestic AML/ATF/CPF policy that strictly adheres to and specifically references Bermuda's AML/ATF/CPF laws and regulations, including:

1. **Primacy of Bermuda Standards** - Where the firm is part of a larger international group, it must ensure that the AML/ATF/CPF measures applied in Bermuda are fully compliant with, and specifically reference, Bermuda's acts and regulations. Any group policy adopted must meet or exceed Bermuda's domestic requirements.
2. **Information Sharing Within the Group** - The group's policies and procedures must provide for group-wide sharing of information required for CDD, ongoing monitoring, record keeping, and other ML/TF/PF risk management controls. Group level AML/ATF/CPF functions must receive customer, account and transaction information including unusual transactions and disclosures relating to suspicion of ML/TF/PF from all subsidiaries. Any reliance or outsourcing between group entities must be evidenced by either a reliance agreement or an outsourcing agreement as the case may be.
3. **Confidentiality Safeguards -** Adequate safeguards on the confidentiality and use of information exchanged within the group must be established and maintained and any transfer of personal information in respect of Bermuda residents must be in accordance with the provisions of the Personal Information Protection Act 2016.
4. **Bermuda Reporting Obligations -** Where operational activities are undertaken by employees in other jurisdictions, those employees must be subject to the same AML/ATF/CPF policies and procedures as Bermuda-based employees. All suspicious transactions or activities linked to the Bermuda entity or a Bermuda person must be reported to the Reporting Officer of the Bermuda entity who based in Bermuda.
5. **Higher Standards Apply -** Where a host jurisdiction imposes AML/ATF/CPF standards more rigorous than Bermuda's, the firm must ensure those higher standards are implemented. Accordingly, while the firm may adopt and align with group-wide AML/ATF/CPF policies and procedures, its domestic Bermuda AML/ATF/CPF policy shall always take precedence in ensuring strict compliance with POCA, ATFA, the Regulations, and all associated Bermuda AML/ATF/CPF legislation and guidance. No group policy shall be

applied in a manner that diminishes or overrides the requirements of Bermuda law.

3.18 Changes in Key Personnel and Beneficial Ownership

In the event of changes to the beneficial ownership of the firm or the key personnel listed below, the firm must notify the Board via email to the Technical Officer within five working days of such change:

i. Director(s);

ii. Compliance Officer;

iii. Reporting Officer; and

iv. Chief Financial Officer.

CHAPTER 4: RISK BASED APPROACH

Regulation 6(3)

4.1 The possibility of being used to assist with money laundering, terrorist and proliferation financing poses many risks for firms including:

i. criminal prosecution under the AML/ATF/CPF legislation;

ii. disciplinary sanctions imposed by CPAB and/or the Board;

iii. civil liability under the Supervision and Enforcement Act; and

iv. damage to reputation leading to loss of business.

4.2 These risks must be identified, assessed and mitigated in the same way as for all business risks faced by a firm. Firms should develop a risk profile for their business which:

i. recognizes that the money laundering, terrorist and proliferation financing threats to a firm vary across clients, jurisdictions, services and delivery channels;

ii. allows a firm to differentiate between clients in a way that matches risk in a particular business;

iii. while establishing minimum standards, allows a firm to apply its own approach to systems and controls, and other arrangements in particular circumstances; and

iv. helps to produce a more cost-effective system.

4.3 The Regulations require a firm to conduct (and keep up to date) a risk assessment, which considers the firm's activities and structure and concludes on the business' exposure to money laundering, terrorist and proliferation financing risk. The Regulations also require a firm to use the outcome of this risk assessment in the development of appropriate risk management systems and controls, and the business' policies and procedures.

4.4 The 2024 National Risk Assessment rated the accounting sector as MEDIUM-LOW for money laundering risk (combining Low threat with Medium vulnerability) and LOW for terrorist financing risk. RPFs should use these national risk ratings as a baseline when conducting their own firm-level risk assessments, while recognizing that individual firm risk profiles may differ based on their specific client base, services, and geographic exposure.

4.5 In particular, a firm is required to develop CDD procedures that take into account risk, and to apply the appropriate CDD measures commensurate to that level of risk. See Chapter 5 Client Due Diligence

4.6 Firms can decide for themselves how to carry out their risk assessment, which may be simple or sophisticated depending on the nature of the firm and its business. Where the business is simple, involving few service lines, with most clients falling into similar categories, a simple approach may be appropriate for most clients, with the focus being on those clients that fall outside the norm.

4.7 Systems and controls will not detect and prevent all money laundering, terrorist or proliferation financing. A risk-based approach will, however, serve to balance the cost burden placed on individual firms and on their clients with a realistic assessment of the threat of a firm being used in connection with money laundering, or terrorist or proliferation financing by focusing effort where it is needed and has most impact.

4.8 An effective and documented risk-based approach will enable a firm to justify its position on managing money laundering, terrorist and proliferation risks to law enforcement, the courts, regulators and supervisory bodies.

4.9 The risk-based approach does not apply to reporting suspicious activity. The Regulations lay down specific legal requirements not to engage in certain activities and to make reports of suspicious activities once a suspicion or reasonable grounds for suspicion is held. However, the risk-based approach does apply to ongoing monitoring of clients and retainers which enable firms to identify suspicions.

4.10 Considering the conclusions of the risk assessment, senior management must organize and control its affairs effectively and be able to demonstrate the existence of adequate risk management systems and controls. A firm may extend its existing risk management systems to address money laundering, terrorist and proliferation financing risks.

Proliferation Financing Risk Assessment

4.11 For the purposes of the risk-based approach, proliferation financing ("PF") risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations related to terrorism and proliferation financing referred to in FATF Recommendation 7. The PF risk assessment can be integrated into the firm's existing ML/TF risk assessment framework without the need to create separate processes.

4.12a Firms must identify and assess their exposure to PF risks by considering:

i. whether clients or beneficial owners have connections to jurisdictions subject to comprehensive sanctions for proliferation (North Korea (DPRK), Iran,);

ii. whether the firm's services could be exploited to facilitate sanctions evasion, including through the creation of shell companies, complex corporate structures, or trust arrangements;

iii. whether transactions involve dual-use goods or technology that could contribute to weapons of mass destruction programmes; and

iv. any other PF risk indicators set out in the FSIU Bermuda CPF Guidance (May 2025)[7].

4.12b The FSIU CPF Guidance identifies the following categories of PF risk indicators that firms should incorporate into their risk assessment:

[7] https://www.gov.bm/sites/default/files/2025-05/Bermuda-CPF-Guidance.1.pdf

i. customer indicators - new customers with connections to blacklisted or sanctioned countries, customers using shell companies or complex structures to obscure beneficial ownership, reluctance to provide information about the nature of business activities;

ii. transaction indicators - payments to or from sanctioned jurisdictions, unusual trade patterns, use of front companies, payments inconsistent with the stated nature of business;

iii. trade-based indicators - transactions involving dual-use goods, misrepresentation of goods on shipping or trade documents, complex shipping routes designed to obscure origin or destination;

iv. country/geographic indicators - FATF black-listed jurisdictions (DPRK, Iran) and jurisdictions subject to comprehensive sanctions regimes present the highest PF risk.

Risk Factors

4.13 The risk assessment will depend on the firm's size, type of clients and the practice area it engages in. In particular, a firm must consider the following risk factors:

i. client risk;

ii. service risk;

iii. delivery channel risk;

iv. geographical risk; and

v. product or transaction risk.

Client risk

4.14 A firm's client diversity can affect the risk of money laundering, or terrorist or proliferation financing. Factors which may vary the risk level include whether a firm:

i. acts for politically exposed persons ("PEPs"), whether inside or outside Bermuda;

ii. acts for clients without meeting them;

iii. acts for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property;

iv. acts for clients that it is, or is not, easy to obtain details of beneficial owners for;

v. acts for entities that have complex ownership structures;

vi. nonprofit organizations;

vii. high net-worth individuals;

viii. client that is conducting a transaction that is not within his or her means based on his stated occupation or income.

Additional factors to consider are:

i. nature and scope of business activities generating the funds/assets. For example, a client engaged in higher risk trading activities or engaged in a business which involves significant amounts of cash may indicate higher risk;

ii. transparency of client. For example, persons that are subject to public disclosure rules, e.g. on exchanges or regulated markets (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g. the Bermuda Stock Exchange, or the BMA may indicate lower risk. Clients where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owners and controllers may indicate higher risk;

iii. secretive clients. Whilst face to face contact with clients is not always necessary or possible, an excessively obstructive or secretive client may be a cause for concern;

iv. reputation of client. For example, a well-known, reputable company, with a long history in its industry, and with abundant independent information about it and its beneficial owners and controllers may indicate lower risk;

v. behavior of client. For example, where there is no commercial rationale for the service that is being sought, or where undue levels of secrecy are requested, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered, may indicate higher risk;

vi. the regularity or duration of the relationship. For example, longstanding relationships involving frequent client contact that result in a high level of understanding of the client relationship may indicate lower risk;

4.15 Firms should prepare a risk profile for clients based on the type of instructions it has received. A client profile should contain sufficient information to enable it to:

i. identify a pattern of expected business activity and transactions within each client relationship;

ii. identify unusual, complex or higher risk activity and transactions that may indicate money laundering, terrorist and proliferation financing activity.

4.16 One of the factors to be considered in undertaking any risk assessment for a client is whether or not the client is acting for a third party or as an intermediary. One or more of the following factors will be relevant when conducting a risk assessment for an introducer or intermediary:

i. the stature and regulatory history of the intermediary or introducer;

ii. the adequacy of the framework to combat money laundering, terrorist and proliferation financing in place in the jurisdiction in which the intermediary or introducer is based;

iii. the adequacy of the supervisory regime to combat money laundering, terrorist and proliferation financing to which the intermediary or introducer is subject;

iv. the adequacy of the measures to combat money laundering, terrorist and proliferation financing in place at the intermediary or introducer;

v. previous experience gained from existing relationships connected with the intermediary or introducer;

vi. the nature of the business conducted by the intermediary or introducer. In this case relevant factors include:

a. the geographic location of the client base;

b. the general nature of the client base, e.g. whether institutional or private client;

c. the risk appetite of the intermediary or introducer;

d. the nature of the services which the intermediary or introducer provides to its clients;

e. whether relationships are conducted by the intermediary or introducer on a face-to-face basis;

f. whether specific relationships are fully managed by the intermediary or introducer; and

g. the extent to which the intermediary or introducer itself relies on third parties to identify its clients and to hold evidence of identity or to conduct other due diligence procedures, and whether such third parties are financial services businesses that are overseen for AML/ATF/CPF compliance in Bermuda or carry out an equivalent business. Whether or not specific intermediary or introduced relationships involve PEP's or other higher risk relationships.

Service Risk

4.17 Firms should consider the different types of risk to which they are exposed within the different service areas that they provide. The risks should be considered within the context that a firm may be used to launder funds or assets through the firm. Factors may include:

i. complicated financial or property transactions;

ii. providing assistance in setting up trusts or company structures which could be used to obscure ownership of property;

iii. payments that are made to, or received from, third parties

iv. payments made by cash;

v. buying and selling business entities; and

vi. managing client assets.

4.18 Specialization within a sector that undertakes higher risk activity from a money laundering, terrorist and proliferation financing perspective will affect the business risk assessment. Examples of higher risk sectors and sensitive business areas for money laundering, terrorist and proliferation financing purposes are:

i. financial services and money services businesses;
ii. high cash turnover businesses (bars and clubs, taxi firms, launderettes, takeaway restaurants, market traders);
iii. gaming and gambling businesses;
iv. real estate and construction;
v. computers and high technology, telecommunications and mobile phone businesses; and
vi. arms and armaments.

4.19 The risks should be considered within the context that a firm may be used to launder funds or assets through the firm. Factors may include:

i. the firm directly handling cash, assets or through payments that are made to, or received from, third parties; or
ii. the firm directly handling the financial affairs, setting up companies, trusts or other structures for politically exposed persons that may be used to obscure beneficial ownership.

Delivery channels risk

4.20 Firms should consider how they interact with their clients and the channels through which it delivers its services to them. Factors may include:

i. the firm acting for clients without meeting them in person;
ii. accepting a client through another firm referral or engagement (such as through an appointed law firm);
iii. transactions that involve third parties;
iv. higher risk payment methods such as cash and virtual assets.

Geographical areas of operation risk

4.21 Business activity in locations with high levels of acquisitive crime, or for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property. Factors may include:

i. FATF black-listed jurisdictions (such as DPRK, Iran, and Myanmar) and jurisdictions subject to comprehensive sanctions regimes (Syria, Russia, Belarus, Libya, Somalia, Yemen, Russian, Venezuela, Afghanistan, Sudan) present the highest geographic risk for proliferation financing and terrorism financing. Firms must give particular attention to any client or transaction connections with these jurisdictions;
ii. acting for clients affiliated to countries with high levels of corruption or organized crime, or where terrorist organizations operate, or countries with inadequate frameworks to prevent and detect money laundering, terrorist and proliferation financing;

iii. in assessing which jurisdictions may present a higher risk, objective data published by FATF[8], World Bank, the Egmont Group of Financial Intelligence Units[9], US Department of State (International Narcotics Control Strategy Report)[10], Office of Foreign Assets Control ("OFAC")[11], Transparency International (Corruption Perception Index) [12] and Basel Institute on Governance, (Basel Index)[13] will be relevant; and

iv. locations with high levels of acquisitive crime.

Product or Transaction

4.22 Specific products or transactions may pose a greater risk of money laundering, terrorist and proliferation financing. Examples transactions that involve private banking, anonymous transactions, and payment received from unknown or unassociated third parties. Additionally, a wide range of products and transactions offered by financial institutions have been found to be vulnerable to abuse. These may be relevant to you if you conduct transactions or manage funds on behalf of clients. These include private banking, retail banking products, correspondent and concentration accounts, transactions with non-client corporate accounts, and wire transfers. Examples of increased risk products and transactions likely to be encountered by Firms:

i. alternative investment/structured products;

ii. trade/export finance;

iii. international private banking;

iv. international correspondent banking;

v. precious metals (delivery) services;

vi. unlimited cards;

vii. benchmark and other setting of indices.

Examples of increased risk transactions:

i. significant/unusual cash/cash like;

ii. pass-through transactions;

iii. nested accounts;

iv. international wires to high-risk countries;

v. suspect shell company transactions;

vi. rapid in/out (high velocity turnover);

[8] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html
[9] https://egmontgroup.org
[10] https://www.state.gov/2025-international-narcotics-control-strategy-report
[11] https://ofac.treasury.gov
[12] https://www.transparency.org/en/
[13] https://baselgovernance.org/basel-aml-index

vii. unusual wire transfers;

viii. smurfing;

ix. dormant accounts that become suddenly active.

Accountancy, audit and insolvency service risk

4.23 Those providing accountancy, auditing or insolvency services will primarily need to consider their risk assessment in respect of the nature of their client base, the business sectors in which their clients operate and the geographical location of their clients. The standing of clients and adherence to sound corporate governance principles will also have an impact including those clients that have previously been prosecuted or fined for criminal or regulatory offences.

4.24 The risk assessment should take account of the following risks:

i. setting up, winding up, or effecting recovery for high cash turnover businesses for clients which may provide a front for criminal money;

ii. being used in an active sense to launder money through the handling of cash or assets or through payments that are made to, or received from, third parties, particularly with a cross-border element;

iii. becoming concerned in an arrangement which facilitates money laundering through the provision of investment services;

iv. becoming a party to serious fraud on the part of senior management or failing to recognize the warning signs relating to management fraud; and

v. the potential for money laundering, terrorist and proliferation financing attaching to the client and/or those who trade with or otherwise interact with clients.

4.25 Those providing accountancy services should also consider the risks when:

i. providing assistance in setting up trusts or company structures which could be used to obscure beneficial ownership of monies and assets settled into trust; and

ii. handling the financial affairs, or setting up companies, trusts or other structures for politically exposed persons whose assets and wealth may be derived from the proceeds of corruption (see section 5 of these Guidance Notes).

Taxation service risk

4.26 Tax practitioners are not required to be experts in criminal law, but they are expected to be aware of the offences which can give risk to the proceeds of crime. For example, the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law. The main areas where offences may arise which might enhance the risks of the tax practitioner becoming concerned in an arrangement are:

i. tax evasion, including making false returns (including supporting documents) accounts or financial statements or deliberate failure to submit returns;

ii. deliberate refusal to correct known errors; and

iii. fraudulent or dishonest conduct.

Summary

4.27 A firm may demonstrate that it has considered its exposure to money laundering, terrorist and proliferation financing risk by:

i. involving all members of senior management in determining the risks posed by money laundering, terrorist and proliferation financing within those areas for which they have responsibility;

ii. considering organizational factors that may increase the level of exposure to the risk of money laundering, terrorist and proliferation financing, e.g. business volumes and outsourced aspects of regulated activities or compliance functions;

iii. considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation;

iv. considering who its clients are and what transactions they do;

v. considering whether any additional risks are posed by the jurisdictions with which the firm or its clients (including intermediaries and introducers) are connected;

vi. considering how the firm establishes business relationships and delivers services or products to its clients. For example, risks are likely to be greater where relationships may be established remotely; and

vii. considering the characteristics of its service areas and assessing the associated vulnerabilities posed by each service area, including delivery channels. For example:

a) the use of third parties such as group entities, introducers and intermediaries to conduct elements of the CDD process;

b) assessing how legal entities and structures might be used to mask the identities of the underlying beneficial owners; or

c) considering how the firm establishes and delivers services to its clients. For example, risks are likely to be greater whether relationships may be established remotely (non-face-to-face).

Risk Mitigation

4.28 Risk mitigation is a core component of the risk-based approach and refers to the implementation of measures designed to limit the potential for money laundering, terrorist and proliferation financing (ML/TF/PF) risks identified by firms, while remaining within its established risk tolerance. Under a risk-based approach, the nature and extent of mitigation measures should be proportionate to the level of risk identified. Where higher

ML/TF/PF risks are identified through the risk assessment process, the accounting firm is required to develop and maintain written risk mitigation strategies. These strategies should consist of clearly defined policies and procedures tailored to address elevated risks and must be applied consistently in higher-risk situations. Examples of appropriate mitigation measures for higher-risk scenarios are provided in Annex 1.

4.29 To be considered effective within a risk-based framework, risk mitigation strategies should be formally documented, ensuring they can be communicated clearly to management and staff. Documentation supports consistency in application and provides evidence of compliance. Reporting entities must also demonstrate that these strategies are actively implemented in practice, with records maintained to show that mitigation measures have been applied in relevant cases.

4.30 Senior management plays a critical role in ensuring the effectiveness of the risk-based approach. Risk mitigation strategies should be approved by senior management and reviewed at least every two years to ensure they remain appropriate and responsive to evolving risks. Ongoing engagement from senior leadership reinforces a strong compliance culture. These strategies must also be communicated to all relevant employees so that staff understand and are able to apply the required mitigation measures in their day-to-day activities.

Ongoing Monitoring

4.31 Ongoing monitoring is another key component of the risk-based approach and complements both risk assessment and risk mitigation activities. Firms are required to monitor financial transactions on an ongoing basis, with the level and intensity of monitoring proportionate to the ML/TF/PF risks identified in the entity's risk assessment. The primary purpose of ongoing monitoring is to detect unusual or suspicious transactions and activities that may indicate potential ML/TF/PF.

4.32 Within a risk-based framework, Firms should establish policies, controls, and procedures that clearly define how monitoring is conducted. This includes specifying the types of transactions or relationships subject to monitoring, the frequency of monitoring activities, the methods used to review transactions, and how monitoring processes are applied consistently across the organization. These policies should also outline how suspicious transactions are identified and escalated. Additional guidance on monitoring obligations is provided in Chapter 6 of these Guidance Notes.

4.33 Monitoring approaches may be manual or automated, depending on the size, nature, and complexity of the reporting entity. Smaller firms may rely on manual processes, while larger or more complex organizations are generally expected to implement automated systems due to higher transaction volumes and increased risk exposure.

4.34 An effective risk-based monitoring framework includes the establishment of a documented monitoring schedule, supported by appropriate management oversight and approval. Firms should also have processes in place to identify and document changes in client behavior or

transaction patterns that deviate from expected activity, with clear escalation procedures for further review where necessary.

4.35 Monitoring parameters or thresholds should be defined to identify transactions that require additional scrutiny, with more frequent and enhanced monitoring applied to higher-risk transactions and business relationships. Ongoing monitoring should also consider the purpose of the business relationship and the expected source of funds established at the outset, ensuring that transactions remain consistent with the client's known profile.

4.36 Where monitoring activities identify suspicious transactions, Firms are required to report these to the FIA in accordance with applicable legal obligations. While the number of SARs submitted may vary depending on the risk profile of the entity, the ability to detect and report suspicious activity remains a key indicator of an effective risk-based monitoring program.

CHAPTER 5: CLIENT DUE DILIGENCE (CDD)

Regulation 5

Regulation 6

Regulation 10

Regulation 11

5.1 Regulation 5 sets out the meaning of client due diligence. The minimum CDD measures required involve:

i. identifying the client or prospective client and verifying the client's identity based on documents, data or information obtained from a reliable and independent source;

ii. identifying, where there is a beneficial owner who is not the client, the beneficial owner (including the settlor of any trust) and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the accountant is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement, including the settlor of any trust;

iii. in the case of a legal entity or legal arrangement, identifying the name and verifying the identity of the relevant natural person having the position of chief executive or a person of equivalent or similar position, including the settlor of any trust;

iv. in the case of a legal entity, identifying and verifying the identity of a natural person (either client, beneficial owner, person of control or ownership) by some means and, where no natural person has been identified, identifying a relevant natural person holding the position of a chief executive; or a person of equivalent or similar position; and

v. obtaining information on and taking steps to understand the purpose and intended nature of the business relationship.

Identification

5 .2 A firm identifies a client by obtaining a range of information about that client. A firm verifies a client's identity by comparing information obtained from the client against documents, data or information obtained from reliable and independent sources.

5.3 The meaning of the term 'client' should be inferred from the definitions of 'business relationship' and 'occasional transaction', the context in which it is used in the Regulations and its standard dictionary meaning.

5.4 A client is generally the natural person or persons with whom a business relationship is established or for whom a transaction is carried out.

5.5 For the purposes of CDD, a natural person's identity comprises information that cannot change (e.g., date and place of birth) and information that may change and accumulate over

time (e.g., name, addresses, family circumstances, employment, positions of authority and physical appearance). To the extent that information concerning identity is available online or in electronic databases, such information may be referred to as an 'electronic footprint'.

5.6 Identifying clients and verifying identity is generally a cumulative process, requiring more than one document or data source to verify all necessary components. Firms should be prepared to accept and verify a range of documents and data.

5.7 A firm must utilize a risk-based approach to determine the extent of identity information or evidence it requests and verifies. In making its determinations, a Firm should consider factors such as:

i. the nature of the product or service sought by the client;

ii. the nature of any other products or services to which the client may migrate without further identity verification;

iii. the nature and length of any existing or previous relationship between the client and the Firm;

iv. the nature and extent of any assurances from other Firm's that may be relied upon; and

v. whether the client is physically present.

5.8 Documentation purporting to offer evidence of identity may emanate from several sources. Documents differ in their integrity, reliability and independence. Some documents are issued after due diligence on a natural person's identity has been undertaken; others are issued upon request, without any such checks being carried out. There is a broad hierarchy of documents:

i. first and foremost, certain documents issued by government departments and agencies or by a court; then

ii. certain documents issued by other public sector bodies or local authorities; then

iii. certain documents issued by RFIs in the financial services sector; then

iv. certain documents issued by other RFIs subject to the Regulations or equivalent legislation;

v. certain documents issued by other organizations.

5.9 Wherever possible, firms should seek documents at the highest level of the hierarchy. To provide the highest level of confidence in a natural person's identity, an identification document should contain a photo of the natural person, and it should be issued by a government department or agency that is known to carry out due diligence prior to issuing the document.

5.10 Regulation 6 specifies the stage at which client due diligence measures should be applied to beneficiaries of: (a) trust; and (b) life insurance policies. Additionally, it requires relevant business persons to determine the extent of client due diligence measures to be applied on a risk sensitive basis, dependent on the geographic areas, services, delivery

channels product or transaction and makes provision for the prohibition against performing client due diligence where doing so may result in the tipping off of another person, which is likely to prejudice an investigation or proposed investigation. Where a relevant person is unable to perform client due diligence in accordance with the above paragraph, he shall, in lieu, file the necessary disclosure with the FIA.

5.11 Regulation 6(1) states that a relevant person must conduct CDD measures when it:

i. establishes a business relationship (where the relationship is expected to have some duration); or

ii. carries out occasional transactions (i.e. a transaction (carried out other than as part of a business relationship) amounting to $15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked);

iii. suspects money laundering, terrorist and proliferation financing; or

iv. doubts the veracity or adequacy of the documents or information previously obtained for the purpose of identification or verification.

5.12 Regulation 6(2) states that a relevant person must apply client due diligence measures at appropriate times to existing clients on a risk sensitive basis.

5.13 Regulation 6(3) requires that a relevant person must:

i. determine the extent of client due diligence measures on a risk sensitive basis depending on the type of client, business relationship, geographic areas, services, delivery channels, product or transaction; and

ii. be able to demonstrate to its supervisory authority the extent of client due diligence measures is appropriate in view of the risks of money laundering, terrorist and proliferation financing.

5.14 Regulation 6(1A) requires that, subject to Regulation 6(1) (described above, in the case of a trust or life insurance policy, a relevant person shall apply client due diligence measures on a beneficiary as soon as the beneficiary is designated for a beneficiary that is identified as a specifically named natural person, legal entity or legal arrangement, taking the name of the person, entity or arrangement. For a beneficiary that is designated by characteristics or by class, obtaining sufficient information concerning the beneficiary to satisfy the relevant person that it will be able to establish the identity of the beneficiary at the time of pay-out.

5.15 Where the client is a Bermuda public authority, Regulation 10 does not require satisfactory evidence of identity to be obtained in respect of the public authority or its beneficial owners and controllers.

5.16 A public authority means any designated person or body of persons (whether corporate or unincorporated) required or authorized to discharge any public function under any Act of the Legislature of Bermuda, or under any act of the Parliament of the United Kingdom which is expressed to have effect, or whose provisions are otherwise applied, in respect of Bermuda, or under any statutory instrument.

Enhanced Due Diligence

5.17 Regulation 11(1) requires that a firm must apply EDD measures on a risk sensitive basis in any situation which by its nature can present a higher risk of money laundering, terrorist or proliferation financing. This may arise in situations where the client has not been physically present for identification purposes and when it is determined that a client is Politically Exposed Person ("PEP"). Where a relationship or transaction is assessed as presenting a higher risk, a firm may demonstrate that it has applied EDD to the higher risk client relationships where it undertakes one or more of the measures set out below. The nature of the measures to be applied will depend on the circumstances of the relationship or transaction and the factors leading to the client relationship being higher risk. Where a relationship or transaction involves a PEP then it must always be considered to present a higher risk.

In addition to the situations described above, enhanced due diligence must be applied where a person or transaction is connected to jurisdictions subject to targeted financial sanctions for the prevention of proliferation of weapons of mass destruction as well any client or situation that you have identified as higher risk in your business risk assessment. A list of risk mitigation measures that can be applied as part of your enhanced due diligence can be found at Annex 1.

Definition of PEP[14]

5.18 A PEP is defined by Regulations (6), (7), 11(s) and 11(6A) as a person who is or has at any time in the preceding year in any country or territory inside or outside Bermuda

i. variously been entrusted with prominent public functions, including those listed in paragraph 2(1)(a) or 2(3) of the Schedule to the Regulations;

Individuals who are or have been entrusted with prominent public functions include the following:

(a) heads of state, heads of government, ministers and deputy or assistant ministers;

(b) members of parliaments;

(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;

(d) members of courts of auditors or of the boards of central banks;

(e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; and

(f) members of the administrative, management or supervisory bodies of state-owned enterprises;

[14] Fims may review FATF Recommendation #12 for additional information on CDD for PEP's

ii. is an immediate family member of such persons, being spouses, partners, children (and the spouses or partners of those children; or

iii. is a known close associate of a person holding a prominent public function including a person who falls in either of the categories listed in paragraphs 2(1)(e) or 2(3)(e) of the Schedule, which includes the following any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person holding a prominent public function; and any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person holding a prominent public function.

Scope of PEPs

5.19 Subsections 2(1) and 2(3) of the Schedule to the Regulations provide for classes of specified politically exposed persons as well as a description of certain other persons who are deemed to be politically exposed persons, along with their relatives and other related parties as set out below:

Outside Bermuda

5.20 Individuals who are or have been entrusted with prominent public functions at both domestic and international level including per 5.18 above. This list does not include middle ranking or more junior officers.

5.21 A further category of PEPs outside Bermuda is members of the administrative, management or supervisory bodies of State-owned enterprises (but not including their spouses, partners, children or associates).

Inside Bermuda

5.22 The 2015 Amendment Act introduced a class of Bermudian officials who have been designated as PEPs for the purposes of Regulation 11(6A), being individuals who are or have been entrusted with prominent public functions and including the following:

i. The Governor, Premier, Ministers and Junior Ministers;

ii. Members of the Legislature;

iii. Permanent Secretaries;

iv. Judges of the Supreme Court and Court of Appeal and Magistrates;

The above categories do not include middle-ranking or more junior officials, but do include, where applicable positions at domestic and international levels.

5.23 The other categories of Bermuda PEPs are:

i. Members of the Board or senior management of the Bermuda Monetary Authority and the Bermuda Regulatory Authority;

ii. Commissioned Officers in the Royal Bermuda Regiment and senior officers above the rank of Sergeant (which includes the Commissioner of Police) of the Bermuda Police Service; and

iii. Members of the Board of Directors and the Chief Executive Officer (by whatever name called) of Bermuda Government owned or controlled enterprises or authorities, including but not limited to:

(a) the West End Development Corporation;

(b) the Bermuda Land Development Corporation;

(c) the Bermuda Development Agency;

(d) the Bermuda Tourism Authority;

(e) the Bermuda Deposit Insurance Corporation; and

(f) the Bermuda Casino Gaming Commission.

5.24 Individuals who have or have had a high political profile, or hold or have held public office, can pose a higher money laundering, terrorist and proliferation financing risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the client or the beneficial owner, into a higher-risk category.

5.25 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year; firms are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriately enhanced monitoring of his transactions or activity at the end of this period. In many cases, a longer period might be appropriate, to ensure that the higher risks associated with the individual's previous position have adequately abated.

5.26 Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Immediate family members include:

i. a spouse;

ii. a partner (including a person who is considered by national law as equivalent to a spouse);

iii. children and their spouses or partners; and

iv. parents.

Persons known to be close associates include:

i. any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or;

ii. any other close business relations, with a person who is a PEP; and

iii. any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

5.27 For the purpose of deciding whether a person is a known close associate of a PEP, the firm needs only to have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose active research by the firm. Firms are required, on a risk-sensitive basis, to:

i. have appropriate risk-based procedures to determine whether a client is a PEP;

ii. obtain appropriate senior management approval for establishing a business relationship with such a client;

iii. take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and

iv. conduct on-going monitoring of the business relationship.

Risk-based procedures

5.28 Firms must utilize risk-based procedures to determine whether the customer or beneficial owner is a PEP in or from Bermuda or a PEP in or from a country or territory outside Bermuda.

5.29 The risk of handling the proceeds of corruption or becoming engaged in an arrangement that is designed to facilitate corruption, is greatly increased where the arrangement involves PEP. Appropriate risk-based systems and controls must be put in place to determine whether a:

i. client;

ii. owner or controller of a client; or

iii. third party on whose behalf a client acts, is a PEP.

Such systems and controls must recognize that clients may subsequently acquire PEP status.

5.30 A firm may demonstrate that it has appropriate systems and controls for determining whether applicants for business or clients are PEPs where it:

i. establishes who are the current and former holders of prominent public functions within those higher risk countries and determines, as far as is reasonably practical, whether or not applicants for business and clients have any connections with such individuals (including through immediate family or close associates);

ii. in determining who are the current and former holders of prominent public functions, it may have regard to information already held by the firm and to external information sources such as the United Nations ("UN"), the European Parliament, the UK Foreign and Commonwealth Office, the Group of States Against

Corruption, and commercially available databases; and exercises vigilance where applicants and clients are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or arms sales.

5.31 Firms should remember that new and existing clients may not initially meet the definition of a PEP but may subsequently become one during a business relationship. The firm should, as far as practical be alert to public information relating to possible changes in the status of its clients regarding political exposure. When an existing client is identified as a PEP, enhanced client due diligence must be applied to that client.

Senior management approval

5.32 Once a PEP has been identified senior management approval to conduct the transaction or continue the business relationship must be obtained. Obtaining approval from senior management for establishing a business relationship does not mean obtaining approval from the Board of directors (or equivalent body), but from the immediately higher level of authority to the person seeking such approval.

Source of wealth and source of funds

5.33 Firms must take reasonable measures to establish both the source of wealth and the source of funds of the PEP. The source of wealth refers to the origin of the individual's total net worth, while the source of funds relates to the specific origin of the funds involved in a particular transaction or business relationship. Information on the source of wealth should indicate the person's volume of wealth and a general understanding of how the person acquired that wealth.

5.34 Information concerning source of funds should be substantive and go beyond the financial institution and account from which the funds were transferred to include details such as the identity of the sender (or recipient) and the reason for sending (or receiving) the funds.

5.35 These measures are intended to ensure that the funds are derived from legitimate activities and to mitigate the heightened risk of money laundering, corruption, or misuse of public office associated with PEPs. The extent and depth of verification should be proportionate to the level of risk identified and may include obtaining information directly from the client, as well as using reliable and independent sources where appropriate. Firms should document the information obtained and the steps taken to verify it, and should apply ongoing monitoring to ensure that transactions remain consistent with the known profile of the PEP.

5.36 Where researching and verifying the accuracy of a person's declaration of the 'source of wealth' or 'source of funds', firms may rely upon a wide range of sources to reveal information about the person's wealth, income, specific assets and lifestyle. Possible sources include databases concerning legal and beneficial ownership, such as publicly available property registers, land registers, asset and income disclosure registers and company registers, as well as past transactions (for existing customers) and internet and media searches including social media.

On-going monitoring

5.37 Reporting entities must conduct enhanced ongoing monitoring for business relationships involving politically exposed persons (PEPs) as part of a risk-based approach. Given the higher ML/TF/PF risk associated with PEPs, monitoring should be more frequent and more detailed than for standard-risk clients. This includes reviewing transactions to ensure they are consistent with the PEP's known source of wealth, source of funds, and the stated purpose of the relationship, as well as identifying any unusual or complex activity. Changes in transaction patterns or client behavior should be promptly assessed and, where appropriate, escalated for further review. Ongoing monitoring should be documented, and any suspicious activity identified must be reported to the FIA in accordance with applicable requirements. General guidance on the on-going monitoring of the business relationship is given in section 6 of these Guidance Notes.

5.38 The Bermuda Economic Investment Residential Certificate, ("EIRC") Holder.

This is a residency-by-investment program requiring a minimum BD$2.5 million (or US$2.5 million) investment to secure immediate, indefinite residency. It allows high-net-worth individuals to live, work and bring families to Bermuda, stimulating economic growth through investments like real estate or local business. In the event firms engage in "specified activities" for EIRC holders, the firms should deem these holders as high risk and apply EDD procedures. If the EIRC holders are PEPs, the EDD described above should also be applied.

Simplified Due Diligence

5.39 As a general rule concerning any business relationship or occasional transaction, firms must apply the full range of CDD measures, including the requirements to identify and verify the identity of the customer, the ownership and control structure of the customer, beneficial owners, the person having the position of chief executive or similar or equivalent position and any other persons with an ownership or controlling interest in the customer, or persons who otherwise exercise significant influence or control over the customer or its business relationship with the firm.

5.40 The circumstances where SDD can be applied are where the client is:

i. itself an AML/ATF/CPF regulated financial institution subject to the Regulations or is a foreign AML/ATF/CPF regulated financial institution subject to requirements equivalent to the Regulations in force in Bermuda and which is supervised for compliance with those requirements;

ii. a company listed on an appointed stock exchange;

iii. an independent professional where the product is an account into which monies are pooled provided that where the pooled account is held in a country or territory other than Bermuda - that country or territory imposes requirements to combat money laundering, terrorist and proliferation financing which are equivalent to those laid down in the Regulations; the independent professional has effectively implemented those requirements; and the independent professional is supervised in that country

or territory for compliance with those requirements; and information on the identity of the person on whose behalf monies are held is available on request to the institution acting as custodian for the account;

iv. a public authority in Bermuda;

v. the product is a life insurance contract where the annual premium is no more than $1,000 or where a single premium of no more than $2,500 is paid for a single policy; or an insurance contract for the purpose of a pension scheme where the contract contains no surrender clause and cannot be used as collateral; or a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

vi. the product and any transaction related to such product fulfils all the conditions set out in paragraph 1 of the Schedule to the Regulations.

5.41 As part of a risk-based approach, SDD measures should be proportionate to the reduced level of risk and may include obtaining less extensive identification information, omitting verification or verifying identity using fewer or more streamlined steps, and reducing the frequency or intensity of ongoing monitoring. However, Firms must still obtain sufficient information to identify the client and understand the nature and purpose of the business relationship. The rationale for applying SDD should be documented, including the factors supporting the low-risk classification. SDD must not be applied where there is suspicion of ML/TF or where higher-risk factors are present, and Firms should remain alert to any changes in risk that would require the application of standard or enhanced due diligence measures.

Verification

5.42 Where seeking to verify identity using documentary evidence, a firm should use reliable, independent source documents, data or information. Where using documentary evidence to verify identity of a natural person, a firm is recommended to use either a valid government-issued document, such as a passport, national identity card or drivers license that incorporates the natural person's full legal name and photograph and one of the following:

i. principal residential address,

ii. date of birth,

iii. place of birth; or

iv. nationality.

5.43 A firm may accept a government-issued document lacking a photograph, such as a birth certificate, which incorporates the natural person's full legal name. In addition, the firm must increase the level of reliability and corroborative value of the documents with one or more additional documents as set out below;

5.44 Where any additional document is used for the purposes of verification, it must incorporate the natural person's full legal name and cumulatively provide both of the following:

i. principal residential address; and

ii. date of birth.

5.45 The document should be government-issued or issued by a judicial authority, a public sector authority, a utility company or a regulated financial institution (RFI) in Bermuda or in a jurisdiction that imposes equivalent AML/ATF/CPF requirements. Examples of other acceptable supporting documents include:

i. instrument of a court appointment (such as liquidator or grant of probate);

ii. current land tax demand letter, bill or statement;

iii. current bank statements, or credit/debit card statements, issued by a Bermuda RFI or an institution in a jurisdiction that imposes equivalent AML/ATF/CPF requirements, provided the document is not printed from the internet; and

iv. utility bill.

The examples of other documents are intended to support the verification of a customer's address **within three months of the verification date**.

5.46 Verification methods provide evidence of identity from several sources. These sources may differ in their integrity, reliability and independence. For example, some identification documents are issued after due diligence on an individual's identity has been undertaken, for example passports and national identity cards; others are issued on request, without any such checks being carried out. A firm should recognize that some documents are more easily forged than others.

5.47 Firms may assess the degree to which they are satisfied with a customer's identity by corroborating information supplied by the customer against information in an electronic database. The greater the depth, breadth and quality of the data held on a customer in a particular electronic database, the more useful the electronic database will be for the purposes of corroborating the information supplied by a customer.

5.48 Several electronic databases provide online access to Firms seeking a primary interface for the purposes of verifying identity. Electronic databases may provide access to positive and negative information concerning a natural person. Although electronic databases can be used, firms may choose to simply request information directly from the client.

5.49 When applying reasonable measures to the re-verification of identity following a change in a particular aspect of identity, e.g. a change of address, a firm may apply a risk-based approach which focuses on higher risk clients.

TIMING OF VERIFICATION

Regulation 8

5.50 A firm must apply CDD measures when it:

i. establishes a business relationship;

ii. carries out an occasional transaction in an amount of $15,000 USD 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;

iii. suspects ML/TF/PF; or

iv. doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

5.51 General rule, firms must always identify the customer and any beneficial owners, the nature of the customer's business, the purpose and intended nature of the business relationship and, where required, the source of funds before the establishment of a business relationship or the carrying out of an occasional transaction.

5.52 Subject to the exceptions referred to below, firms must verify the identity of the customer and any beneficial owners before establishing a business relationship or carrying out an occasional transaction.

5.53 Exception: where performing CDD measures may tip-off a customer or potential customer where there is suspicion that a transaction relates to ML/TF and a person associated with a firm believes that performing CDD may tip off the customer or potential customer to that suspicion, the person must not perform the CDD measures, and, in lieu, the firm must file a SAR with the FIA.

5.54 Exception: for life insurance and trust beneficiaries- the identification and verification of a trust customer or life insurance policy customer must be completed before establishing the business relationship. Identification of the identity of a beneficiary of a trust or life insurance policy must take place as soon as the beneficiary is designated. Verification of the identity of the beneficiary under a trust or life insurance policy may take place later but must be satisfactorily complete at the time of any payment to the beneficiary and at the time the beneficiary seeks to exercise any right or power of control vested under the trust arrangement or life insurance policy.

5.55 Exception: where essential to avoid interrupting normal conduct of business - on an exceptional basis and only where the risk of ML/TF/PF has been assessed as low, firms may verify the identity of the customer and any beneficial owners during the establishment of a business relationship, provided that the following safeguards are put in place:

i. ensuring that the exception is essential to avoid interrupting normal conduct of business;

ii. establishing that there is little risk of ML/TF/PF occurring and that any ML/TF/PF risk that may arise is effectively managed;

iii. completing the verification as soon as practicable after the initial contact;

iv. ensuring that the business relationship or account is not closed prior to efforts to complete verification;

v. ensuring that funds received are not passed to third parties or the account holder prior to the satisfactory completion of verification;

vi. imposing, using a risk-based approach, limits on the number, types and/or amount of transactions that may be carried out prior to the completion of verification; and

vii. monitoring, using a risk-based approach, by senior management of the first and each subsequent transaction until verification has been completed.

This exception may pertain to low-risk types of non-face-to-face business and high-speed securities transactions through a recognized stock exchange.

5.56 As it takes time to form a trust, the time required for trust service providers to verify identity is not considered interruptive of normal business and, as a result, this exception is not available to those service providers.

5.57 Firms must satisfy themselves that the primary motive for the use of these exceptions is not for the circumvention of CDD procedures. Where there is knowledge, suspicion or reasonable grounds for suspicion of ML/TF/PF, these exceptions are not available. Where a new business relationship is assessed as posing a higher risk, these exceptions are not available and enhanced due diligence is required.

Insolvency Practitioners

5.58 In very limited circumstances (for example a hostile appointment), it may not be possible to have completed the identification and verification procedures before taking office. In these circumstances firms should gather sufficient information to allow them to form a general understanding of the identity of the debtor, company officers or beneficial owners of the entity, including information about what the business did and where it traded, in order that that the risk of ML/TF/PF can be assessed. Information from online or subscription services may be a useful source of material for CDD, but firms need to be satisfied that the information is reliable and up to date.

5.59 In cases where a firm is appointed without any prior contact with the debtor, company officers or beneficial owners of the insolvent entity (such as appointments made via a creditors' decision procedure where an alternative firm is nominated by the creditors, or an appointment made as a result of a creditor's petition), firms should complete their CDD procedures as soon as is practicable on appointment (within five working days is considered a reasonable period). Much of the necessary information may be obtainable from the firm who assisted with convening the decision procedure, or where appropriate, from a prior office holder. In situations where management of the client entity are hostile, and unwilling to provide further information, the firm should review other sources of

publicly available information to enable reasonable verification of the client within the required timescale.

Keeping information current

5.60 Firms must review the documents, data and information they hold in relation to a customer to ensure that the records are up to date, adequate and relevant to the business relationship or transaction. Once a firm has verified the identity of a customer and any beneficial owners, it should re-verify where:

i. doubts exist as to the veracity or adequacy of the evidence previously obtained for the purposes of identifying and verifying the customer and any beneficial owners;

ii. there is knowledge, suspicion or reasonable grounds for suspicion of ML/TF/PF in relation to the customer;

iii. the customer's activities are inconsistent with the firm's understanding of the customer's business or the purpose and intended nature of the business relationship;

iv. there is a material increase in the risk rating assigned to the customer or to the products, services, delivery channels, or countries or geographic areas with which the customer engages;

v. other trigger events, such as an existing customer applying to open a new account or establish a new relationship, prompt a firm to seek appropriate evidence.

5.61 Where a firm cannot obtain identification documents that bear a photograph of the customer and match those documents against the customer in a face-to-face setting, the firm should apply additional verification measures to manage the risk of impersonation fraud. The additional measures may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures or may include a combination of:

i. requiring the first payment to be carried out through an account in the customer's name with a firm in Bermuda or a jurisdiction that imposes equivalent AML/ATF/CPF requirements;

ii. verifying additional aspects of the customer's identity or of their 'electronic footprint';

iii. using a reliable, independent digital identification system that is adequately protected against internal and external manipulation or falsification to avoid creating false identities;

iv. requiring copy documents to be certified by an acceptable person;

v. contacting the customer via telephone prior to opening the account on a home or business number, which has been verified (electronically or otherwise), or a 'welcome call' to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;

vi. communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening

documentation to the customer, which in full or in part, is required to be returned, completed or acknowledged without alteration);

vii. requiring internet sign-on following verification procedures, where the customer uses security codes, tokens and/or other passwords that have been set up during account opening and provided by mail (or secure delivery) to the named natural person at an independently verified address; and

viii. employing other reasonable card or account activation procedures.

CERTIFICATION OF DOCUMENATION

5.62 For certification to be effective, the certifier will need to have seen the original documentation and, where documents is to be used to provide satisfactory evidence of identity for an individual, have the meet individual. An acceptable certifier will also be subject to professional rules providing for the integrity of their conduct.

Persons certifying document must certify that:

i. they have seen original documentation verifying identity and or residential address;

ii. the copy of the document is a complete and accurate copy of the original

5.63 The certifier must also sign and date the copy document and provide adequate information to be contacted for verification. The certification should include the name, position, capacity and their address and telephone number or email address to be contacted.

Acceptable persons and certification process as an example;

5.64 A copy of a document presented in lieu of examining the original document must bear an original certification by individual holding one or more of the following professional positions:

- a qualified accountant, registered with the relevant national professional body;
- a qualified actuary, registered with the relevant national professional body;
- a qualified lawyer, attorney or barrister, registered with the relevant national professional body;
- Commissioner of Oaths;
- a qualified doctor, registered with the relevant national professional body;
- a serving judge;
- a serving Justice of the Peace;
- a current Member of Parliament (all Houses) or Local Government Officer;
- Notary Public;

- officer of an embassy, consulate or high commission of the country or territory that issued the passport or I.D.

5.64a It is best practice that wherever possible, the professional certifying the documents not be the person conducting the CDD or involved in the subsequent engagement.

5.65 The certifier is required to certify all copy documents as follows:

On each photocopied document, the certifier must write:

"I, [name of certifier] confirm that this is a true copy of the original document which I have seen"

For documents containing a photo, the certifier must also write:

"I, [name of certifier] confirm that I have met [name of person whose document is being certified] in person and that the photograph is a true likeness of him / her."

In addition to the above, the certifier must also write his / her:

i. full name;

ii. signature;

iii. occupation;

iv. company / professional address, telephone number and email address;

v. date on which the document was certified.

All certified documents must meet the following criteria:

i. the person signing as a certifier cannot be a relative or family member of the person; and

ii. all copy documents accepted must be clear and legible.

Client Due Diligence update

5.66 Firms must screen all clients and beneficial owners against applicable sanctions lists, including the UK Consolidated List (which serves as Bermuda's sanctions list), and sanctions lists maintained pursuant to the International Sanctions Act 2003 and related regulations. Where a client or beneficial owner is found to be a designated person, the firm must immediately freeze any funds or economic resources and report to the FSIU via a Compliance Reporting Form (CRF). No transaction or business relationship may be entered into or continued with a designated person without an appropriate license from the Governor or relevant authority.

CHAPTER 6: ONGOING MONITORING

Regulation 6

Regulation 7

Regulation 15

6.1 Ongoing monitoring procedures apply to all business relationships, including those with existing clients. Monitoring of existing clients will be based on the type of risk the client represents.

6.2 Regulation 7(1) requires a relevant person to conduct ongoing monitoring of a business relationship. Ongoing monitoring of a business relationship means:

i. scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds or digital asset);

ii. to ensure that the transactions are consistent with the relevant person's knowledge of the client, his business and risk profile;

iii. an investigation into the background and purpose of all complex, unusually large transactions, or unusual patterns of transactions which have no apparent economic or lawful purpose and record the findings in writing; and

iv. so far as practicable keeping the documents, data or information obtained for the purpose of applying client due diligence measures up to date.

6.3 Regulation 6(3) applies to the duty to conduct ongoing monitoring to CDD measures.

6.4 The monitoring procedures must:

i. involve a firm applying its understanding of its business (i.e. the outcome of its risk assessment) to determine the nature of usual activity and its expectations for unusual and higher risk activity and transactions;

ii. be designed to result in the identification of unusual and higher risk activity or transactions;

iii. require that special attention is paid to specific higher risk activity, clients and transactions;

iv. require the examination of any unusual or higher risk activity or transaction by an appropriate person to determine the background and purpose of the activity or transaction;

v. in connection with the above examination, involve the collection of additional information (where appropriate);

vi. establish whether there is a rational explanation (an apparent economic or visible lawful purpose) for the unusual or higher risk activity or transaction, and document these findings in writing; and

vii. result in appropriate action being taken as a result of the findings of the above procedures.

6.5 When conducting monitoring procedures, the following are to be higher risk activity and transactions:

i. complex transactions;

ii. unusual large transactions;

iii. unusual patterns of transactions;

iv. activity and transactions:

(i) connected with jurisdictions which do not, or insufficiently apply the FATF Recommendations; or

(ii) which is the subject of UK, UN or European Union ("EU") countermeasures;

(iii) activity and transactions that may be conducted with persons who are the subject of UK, UN or EU sanctions and countermeasures;

(iv) activity or transactions with PEPs or where PEPs are connected with the client, whether inside or outside Bermuda;

(v) activity or transactions for clients who have not been physically present for identification purposes; and

(vi) activity connected with persons or jurisdictions subject to targeted financial sanctions for the prevention of proliferation of weapons of mass destruction (WMD).

6.6 In line with enhanced due diligence requirements for higher risk clients, more intensive scrutiny of client activity and transactions may involve, for example, periodic re-screening of the entire client base against updated sanctions lists, including the HM Treasury Consolidated List. Firms must ensure that when sanctions lists are updated, existing clients and beneficial owners are re-screened in a timely manner. Screening should be conducted at least when lists are updated and as part of the regular CDD review cycle.

Monitoring for PF Indicators

6.7 During the course of business relationships, firms must monitor for PF indicators, including:

i. unusual connections to sanctioned jurisdictions (DPRK, Iran, Syria, Myanmar);

ii. transactions or business activities involving dual-use goods or technology;

iii. front company structures that may be used to circumvent targeted financial sanctions;

iv. unexplained changes in beneficial ownership that may indicate an attempt to obscure connections to designated persons; and

v. any other indicators set out in the FSIU Bermuda CPF Guidance (May 2025). Where such indicators are identified, the firm must conduct further enquiries and, where appropriate, make a report to the FSIU and/or the FIA:

(i) increase in frequency of reviews and updating of CDD information;

(ii) increased reviews of client activity and transactions against the client's expected activity profile; and

(iii) client reviews being conducted by persons not directly involved in managing client relationships.

How to conduct on-going monitoring

6.8 The examination of unusual and higher risk activity or transactions may be conducted either by fee earners or by accounts or administration staff. In any case, a firm should ensure that the reviewer has access to relevant CDD information, and that the enquiries made and the conclusions reached by the reviewer are appropriate.

6.9 Appropriate follow up action may include:

i. updating CDD information to record the results of the enquiries made;

ii. reviewing the appropriateness of the client risk assessment considering the unusual activity and/or additional CDD information obtained;

iii. applying increased levels of monitoring to relationships; and

iv. where the activity or transaction does not have a rational explanation, considering whether the circumstances require a SAR to be submitted to the firm's Reporting Officer.

6.10 In determining the nature of the monitoring procedures that are appropriate, a firm may have regard to the following factors:

i. its risk assessment;

ii. the size and complexity of its business;

iii. the nature of its legal business and services;

iv. whether it is possible to establish appropriate standardized parameters for unusual activity;

v. the monitoring procedures that already exist to satisfy other business needs and;

vi. the most recent published ML/TF/PF national risk assessment.

vii. the expected frequency, size, and origin/destination of client funds or other activity for individual clients; and

viii. the presence of risk factors specific to the nature of the activity or matter undertaken for the client. A firm should determine risk factors based on its knowledge of its client and should have regard to typologies (whether external or

developed from its own experiences) relevant to the nature of its business activities.

6.11 A firm may demonstrate that it is appropriately examining unusual and higher risk activity and transactions where it:

i. reviews the identified activity/transaction considering the client risk assessment and the CDD information that it holds;

ii. makes further enquiries to obtain any further information required to enable a determination as to whether the activity/transaction has a rational explanation; and

iii. considers the activity or transaction in the context of any other relationships connected with the client.

6.12 Timelines for ongoing monitoring should be clearly defined and documented as part of the firm's policies and procedures. These timelines should reflect the nature, scale, and risk profile of the activities being monitored, ensuring that reviews occur at appropriate and regular intervals. Accountants should establish procedures to assess whether monitoring activities remain effective over time, with provisions for more frequent review where heightened risks or significant changes arise. All monitoring schedules should be communicated to relevant stakeholders and periodically revisited to ensure continued relevance and alignment with regulatory and organizational requirements.

6.13 Risk assessment should be carried out on an ongoing basis for those clients that have been identified as high risk throughout the business relationship and for each instruction. In the case of a client relationship assessed as presenting a higher risk, a firm may demonstrate that its CDD information remains up to date where it is reviewed and updated on at least an annual basis.

6.14 In the case of other relationships, a firm may demonstrate that its CDD information remains up to date where it is reviewed and updated on a risk sensitive basis, including where additional "factors to consider" become apparent (i.e. trigger events - when taking new instructions from a client, or meeting with a client may also present a convenient opportunity to update CDD information).

6.15 Comprehensive understanding of the risk presented by a client relationship may only become evident at a later stage following the establishment of a relationship. A firm may demonstrate that its client risk assessments remain up to date where its monitoring procedures involve consideration as to the ongoing appropriateness of the client's risk assessment.

CHAPTER 7: SUSPICIOUS ACTIVITY AND SANCTIONS REPORTING

Regulation 17

7.1 Regulation 17 requires a relevant person to maintain internal reporting procedures to allow for reports to be made to a Reporting Officer when information comes to the attention of an employee which gives rise to knowledge or suspicion or reasonable grounds for suspicion that another person is engaged in money laundering, terrorist and proliferation financing. The Reporting Officer after considering the information shall disclose that information to the FIA where he knows or suspects or has reasonable grounds to suspect that a person is engaged in money laundering, terrorist and proliferation financing.

7.2 The provisions of Regulation 17 requiring a relevant person to maintain internal reporting procedures however do not apply to sole practitioners.

7.3 Firms are required to make a report in respect of information or any other matter that comes to them during their profession or business where they know or suspect or have reasonable grounds for suspicion that a person is engaged in money laundering, terrorist and proliferation financing.

7.4 In the context of suspicious transaction reporting, suspicion refers to a state of mind where there is a reasonable basis to believe that a transaction or activity may be linked to criminal conduct, such as money laundering or fraud, even if there is no definitive proof. It arises from a combination of facts, patterns, or unusual behaviors that would prompt a prudent professional to question the legitimacy of the activity and consider whether it warrants further review or reporting.

7.5 A transaction which appears unusual is not necessarily suspicious. Even clients with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many clients will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So, the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

7.6 The concept of a suspicion reportable under the AML/ATF/CPF legislation includes having reasonable grounds for suspicion. Being in possession of facts which to a reasonable person would arouse suspicion, whether one has formed any such suspicion, imposes a reporting duty. Thus, the trigger point for reporting has been lowered with corresponding greater obligation on accountants to be aware of a) the facts occurring around them; b) the implication of those facts which others might draw whether they share such interpretation; and c) their duty to report.

Reporting on activities outside Bermuda

7.7 The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal conduct, wherever carried out, that would constitute an

offence if it took place in Bermuda. This broad scope excludes offences which the institution, staff member or Reporting Officer knows, or believes on reasonable grounds, to have been committed in a country or territory other than Bermuda and not to be unlawful under the criminal law then applying in the country or territory concerned. The duty to report under ATFA applies in relation to any terrorist financing offence, under sections 5 - 8 of that act, that would have been an offence under these sections of the act had it occurred in Bermuda.

7.8 The requirement to report knowledge or suspicion or having reasonable grounds for suspicion of money laundering, terrorist and proliferation financing also applies where a Bermuda company or Bermuda partnership conducts business outside Bermuda. Where business is conducted outside Bermuda, for example through an office in another jurisdiction, through business trips to another jurisdiction, or where functions are outsourced to another jurisdiction and knowledge or suspicion or reasonable grounds for suspicion of money laundering, terrorist and proliferation financing arises in respect of that non-Bermuda business, a report must be made to the FIA in the same way as for business conducted in Bermuda. Under the Regulations, where a firm conducts business pertaining to the specified activities in section 49(5) of POCA, but outsources aspects of its activities to another jurisdiction, whether to a group entity or to a third party, its money laundering, terrorist and proliferation financing reporting procedures must also cover those outsourced activities.

7.9 It is likely that there will also be a requirement to report the knowledge or suspicion of money laundering, terrorist or proliferation financing to an overseas financial intelligence unit to avoid the commission of an offence in that jurisdiction. This is known as a dual report requirement.

Reporting Officer

7.10 Regulation 17 requires that accountancy firms (but not sole practitioners) must appoint a Reporting Officer. A firm's Reporting Officer is responsible for ensuring that, when appropriate, the information or other matter leading to knowledge or suspicion of money laundering, terrorist and proliferation financing is reported to the FIA. The decision to report or not to report must not be subject to the consent of anyone else.

7.11 A firm must ensure that the Reporting Officer:

i. is employed by the firm;

ii. is not on the board of directors of the firm (it is recognized that in sole practitoners/partnerships and smaller firms this may be unfeasible);

iii. is based in Bermuda;

iv. has sufficient experience and skills;

v. has appropriate independence;

vi. has a sufficient level of seniority and authority within the business;

vii. has sufficient resources, including sufficient time, and (if appropriate) is supported by Deputy Reporting Officer(s);

viii. can raise issues directly with senior management;

ix. is fit and proper;

x. maintains a record of all enquiries received from law enforcement authorities and records relating to all internal and external SARs;

xi. is fully aware of both their own and the business' obligations under the Regulations, POCA, ATFA, the AML/ATF Guidance Notes and by extension these Guidance Notes;

xii. ensures that relationships are managed effectively post disclosure to avoid tipping-off any third parties; and

xiii. acts as the liaison point with the Board/CPAB/FIA and in any other third-party enquiries in relation to money laundering, terrorist and proliferation financing.

7.12 Whilst the Regulations requires one individual to be appointed as Reporting Officer, given the size and complexity of operations of many firms, it may be appropriate to designate an additional person ("Deputy Reporting Officer") to whom SARs may also be made. Where a firm has appointed one or more Deputy Reporting Officers, it must ensure that the requirements set out above for the Reporting Officer are also applied to any Deputy Reporting Officer. It should be noted that whereas the Reporting Officer must be based in Bermuda, the Deputy Reporting Officer should ideally be based in Bermuda.

7.13 Where a firm has appointed one or more Deputy Reporting Officers, it must ensure that the Reporting Officer:

i. keeps a record of the appointment of all Deputy Reporting Officers;

ii. provides support to and routinely monitors the performance of any Deputy Reporting Officer; and

iii. ensures that SARs are considered and determined in an appropriate and consistent manner.

7.14 In the event that the position of Reporting Officer is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of Reporting Officer at all times, a firm must take action to appoint an appropriate member of senior management to the position on a temporary basis.

Reporting

7.15 Section 44 (assisting another to retain the benefit of criminal conduct) and section 45 (acquisition, possession or use of proceeds of criminal conduct) of POCA states that where a person is concerned in an arrangement involving the proceeds of crime, or has possession of the proceeds of crime, they will not have committed an offence if the disclosure is made before he does the act concerned and the act is done with the consent of the FIA, or the disclosure is made after he does the act but is made on his initiative as soon as it is

reasonable for him to make it. Subsections 43(2) - (5) and 44(3) and 45(5) and (5A) - (5F) of POCA protect persons who carry out transactions that could contravene subsection 43(1) (concealing or transferring criminal property) or subsection 44(1) (assisting another to retain criminal property) or subsection 45(1) (acquisition, possession or use of criminal property) where they have done so having made a disclosure to the FIA and have obtained its consent or deemed consent for the transaction.

7.16 Section 12 of ATFA contains similar provisions in circumstances where offences would otherwise be committed under section 5 (fund-raising), section 6 (use and possession of property), section 7 (funding arrangements) and section 8 (money laundering).

7.17 Section 9 of ATFA contains an offence of failure to report knowledge or suspicion or having reasonable grounds for suspicion of another person's involvement in money laundering, terrorist and proliferation financing (sections 5 to 8 of ATFA), where the knowledge or suspicion or reasonable grounds for suspicion arose during the course of a trade, profession, business or employment, other than in the course of a business in the regulated sector.

7.18 Schedule 1 Part 1 paragraph 1 of ATFA contains a further offence, where a person fails to report another person's involvement in money laundering, terrorist or proliferation financing (sections 5 to 8 of ATFA), where their knowledge or suspicion or reasonable grounds for suspicion, arose during business in the regulated sector.

7.19 There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

7.20 A firm must ensure that:

i. where a new or an existing client fails to supply adequate CDD information, or adequate documentation verifying identity (including the identity of any beneficial owners and controllers or settlor of any trust), consideration is given to making a SAR;

ii. internal reporting procedures encompass the internal recording of attempted transactions and business that has been turned away;

iii. employees make written internal SARs containing all relevant information to the Reporting Officer as soon as it is reasonably practicable after the information comes to their attention in writing;

iv. SARs include as full a statement as possible of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering, terrorist and proliferation financing activity and full details of the client;

v. reports are not filtered out by supervisory staff or managers such that they do not reach the Reporting Officer; and

vi. reports are acknowledged by the Reporting Officer.

7.21 A firm must establish and maintain arrangements for disciplining any member of staff who ails, without reasonable excuse, to make an internal SAR where they have knowledge or suspicion or reasonable grounds for suspicion of money laundering, terrorist or proliferation financing.

7.22 A firm may demonstrate that it has established and maintained appropriate arrangements for disciplining staff, where employment contracts and employment handbooks provide for the imposition of disciplinary sanctions for failing to report knowledge or suspicion or reasonable grounds for suspicion.

7.23 Firms, but not sole practitioners, need to have a system clearly setting out the requirements for making an internal SAR. These may include:

i. the circumstances in which a disclosure is likely to be required;

ii. how and when information is to be provided to the Reporting Officer or deputies;

iii. resources which can be used to resolve difficult issues around making a disclosure;

iv. how and when a disclosure is to be made to the FIA;

v. how to manage a client when a disclosure is made whilst waiting for consent; and

vi. the need to be alert to tipping-off issues.

7.24 firm must ensure that:

i. all relevant information is promptly made available to the Reporting Officer on request to ensure that internal SARs are properly assessed;

ii. each SAR is considered by the Reporting Officer considering all relevant information; and

iii. the Reporting Officer documents the evaluation process following and reasons for the decision to report or not to report to the FIA.

7.25 In order to demonstrate that a report is considered considering all relevant information when evaluating a SAR, the Reporting Officer may:

i. review and consider transactions, patterns and volumes, previous patterns of instructions, the length of the business relationship and CDD information; and

ii. examine other connected accounts or relationships. Connectivity can arise through commercial connections, such as transactions to or from other clients or common introducers, or through connected individuals, such as third parties, common ownership of entities or common signatories. However, the need to search for information concerning connected accounts or relationships should not delay the making of a report to the FIA.

Communication with the FIA

7.26 A firm must ensure that the Reporting Officer files a SAR which contains all the relevant information, including the provision of all the necessary documentation in support of the

SAR, directly to the FIA as soon as is reasonably practicable, in a format approved by the FIA.

Relevant information includes:

i. full details of the client and as full a statement as possible of the information giving rise to knowledge or suspicion or reasonable grounds for suspicion. It will be particularly important to provide as comprehensive a narrative to the FIA as possible describing the who, what, when, where and why of the suspicion;

ii. if a particular type of criminal conduct is suspected, a statement of this conduct;

iii. financial records;

iv. correspondence;

v. file/account opening documentation;

vi. where a firm has additional relevant information that could be made available, the nature of this information; and

vii. statistical information to assist the FIA in its analysis of reports.

7.27 The FIA does not accept manual submissions of SARs (including those faxed or emailed). All SAR filing is done electronically, and to file a SAR you should:

1. register with goAML by filing out a Registration form on the website;
2. obtain your login information;
3. file your SAR(s) online;
4. contact the FIA for any training issues at:

Additional information may be obtained at www.fia.bm

7.28 A SAR must be filed with the FIA as soon as it is reasonably practicable to do so once knowledge or suspicion has been formulated or where there are reasonable grounds for suspicion. As such it must be made either before a transaction occurs, or afterwards, if knowledge or suspicion is formulated, or the grounds for suspicion present themselves, with the benefit of hindsight after a transaction or activity occurs.

7.29 Firms should keep comprehensive records of suspicions, objective facts providing grounds for suspicion, and disclosures because disclosures of a suspicious activity or transaction is a defense to criminal proceedings. Such records may include notes of:

i. ongoing monitoring undertaken and concerns raised by management and staff;

ii. discussions with the Reporting Officer regarding concerns;

iii. advice sought and received regarding concerns;

iv. why the concerns did not amount to a suspicion or meet the objective test of "reasonable grounds" and a disclosure was not made;

v. copies of any disclosures made;

vi. conversations with the FIA, supervisory authorities etc. regarding disclosures made; and decisions not to make a report to the FIA which may be important for the Reporting Officer to justify his position to law enforcement.

Tipping Off

POCA Section 47(1) and ATFA Section 10A

7.30 Where a person knows or suspects or has reasonable grounds to suspect that the police are acting or proposing to act in connection with an investigation which is being or is about to be conducted into money laundering, terrorist or proliferation financing, and discloses any information to any other person which is likely to prejudice that investigation or proposed investigation, they commit an offence. It is a defense if the person does not know or suspect that disclosure is likely to prejudice the investigation.

POCA section 47(2) and ATFA section 10A(2)

7.31 Once an internal or external SAR has been made, it is a criminal offence for any person knowing or suspecting or having reasonable grounds to suspect that such a report has been made, to disclose to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following such a disclosure.

7.32 In order to prevent the commission of a tipping-off offence, at the time of acknowledging receipt of an internal SAR, the Reporting Officer may provide a reminder to the member of staff submitting the report of the risk of communicating information that might prejudice law enforcement enquiries.

7.33 Regulation 6(1)(c) requires a relevant person to apply client due diligence measures when the firm suspects money laundering, terrorist or proliferation financing. Therefore, there is a risk that the contact between the firm and the client (or his advisors) could unintentionally lead to the client being tipped off, where the process is managed without due care. Although it is not tipping off to include a paragraph about a firm's obligations under the money laundering, terrorist and proliferation financing legislation in a firm's standard client care letter. Reference should be made to the client due diligence procedures outlined in section 5 of the Guidance Notes.

7.34 In circumstances where a SAR has been filed with the FIA, and the CDD procedures are incomplete, the risk of tipping-off a client (and its advisers) may be minimized by ensuring that employees undertaking due diligence enquiries are aware of tipping-off procedures and are provided with adequate support, such as specific training or assistance from the Reporting Officer.

Obtaining Consent from the FIA

7.35 Where a SAR is made before a suspected transaction or event takes place, FIA consent must be obtained before the transaction or event occurs. Consent will only be given in

respect of that particular transaction or activity, and future transactions or activity should continue to be monitored and reported accordingly (POCA sections 44(3) and 45(5)(b)(i); and ATFA section 12 sets out consent provisions).

7.36 Where a SAR report is made after the transaction or event, this will be acknowledged by the FIA. In the absence of any instruction to the contrary from the FIA, a firm will be free to maintain the client relationship under normal commercial circumstances. However, receipt of an acknowledgment from the FIA in these circumstances does not indicate that the knowledge or suspicion or ground for suspicion is with or without foundation, and future transactions or activity should continue to be monitored and reported as appropriate.

7.37 Refusal to act upon a client's instruction (for example, as a result of the FIA refusing to give consent for a transaction to proceed) may also lead to civil proceedings being instituted by the client. It may be necessary in circumstances where a client has instigated civil proceedings for a firm to seek the directions of the court.

Transactions following a disclosure

7.38 A firm is not obliged to continue relationships with clients if such action would place them at commercial risk. Termination is ultimately a commercial decision, however, in certain circumstances a firm should consider liaising with the FIA to determine whether it is likely that termination would alert the client, and in such a case the FIA may request that a relationship is not terminated to avoid prejudicing an investigation.

7.39 If a firm, having filed a SAR, wishes to terminate a relationship or transaction and is concerned that in doing so, it may prejudice an investigation resulting from the report, it should seek the consent of the FIA to do so where the activities referred to fall within sections 44 and 45 of POCA and section 12 of ATFA. This is to avoid the danger of tipping-off.

FIA Information Request

7.40 Section 16(1) of the FIA Act provides that the FIA may, in the course of enquiring into a suspicious transaction relating to a money laundering, terrorist and proliferation financing offence, serve a notice in writing on any person requiring that person to provide the FIA with such information as it may reasonably require for the purpose of its enquiry.

7.41 Section 16(2) of the FIA Act provides that a person who is required to provide information pursuant to a notice served under subsection (1) must provide the information to the FIA in such manner as the FIA requires.

7.42 Pursuant to section 16(3) of the FIA Act, any person who without reasonable excuse fails to comply with a requirement imposed on him under this section shall be guilty of an offence and liable on summary conviction to a fine or to imprisonment or to both.

7.43 Nothing in section 16 requires the disclosure of information which is subject to legal professional privilege.

Service of Orders and Notices

7.44 During the course of an investigation, a firm may be served with an order designed to restrain funds or property pending the outcome of an investigation. It should be noted that the restraint order may not apply to all funds or assets involved within a particular business relationship and a firm should consider what, if any, property may be utilized.

7.45 Upon the conviction of a defendant, a court may order the confiscation of their criminal proceeds or the confiscation of assets to a value representing the benefit of their criminal conduct, which may require the realization of legitimately obtained assets. A firm may be served with a confiscation order in relation to any funds or property belonging to that defendant. For example, if a person is found to have benefited from drug dealing to a value of $100,000, then the court may order the confiscation of any assets belonging to that person to a value of $100,000. Confiscation of the proceeds of criminal conduct is becoming commonplace within many jurisdictions, and legislation in place in Bermuda provides a mechanism by which overseas criminal confiscation orders may be recognized. Overseas civil confiscation orders may also be recognized in Bermuda.

Freezing of funds

7.46 Section 15(1) of the FIA Act provides that the FIA may in the course of enquiring into a suspicious transaction relating to the suspected proceeds of criminal conduct or to a money laundering, terrorist and proliferation financing offence serve a notice on any relevant institution in Bermuda requiring it to not make available any funds to any person specified in the notice. Pursuant to section 15(2) of the FIA Act such a notice shall be in writing and may require the relevant institution, as defined by section 2(2), to freeze funds for a period not exceeding 72 hours. A relevant institution commits an offence if without reasonable excuse it fails to comply with a notice served on it under subsection (1) and a relevant institution guilty of an offence under subsection (1) is liable on summary conviction to a fine.

7.47 Under sections 52A(1) and (2) of POCA, a magistrate, upon the application of a police officer in the course of a confiscation investigation or an investigation into money laundering, may make an order requiring a relevant institution, as defined by section 7(2), to not make available the suspected funds to any person. Pursuant to section 52A(3) such an order shall not have effect for more than seven days.

Terrorism and Proliferation Financing Sanctions Reporting

7.48 It is essential for RPFs to understand the distinction between suspicious activity reporting under the AML/ATF/CPF framework and sanctions-related reporting. SARs are filed with the FIA through the goAML electronic platform when there is knowledge, suspicion, or reasonable grounds for suspicion of money laundering, terrorist and proliferation financing. Sanctions-related reports are filed with FSIU using the CRF when a firm identifies a match with a designated person or suspects a breach of sanctions obligations.

7.49 Where a suspicion relates to both potential money laundering, terrorist and proliferation financing and a potential breach of sanctions, dual reports must be made a SAR to the FIA

and a CRF to the FSIU. The obligation to report to the FSIU arises independently of and in addition to the obligation to report to the FIA.

7.50 Firms should implement procedures to conduct targeted financial sanctions screening at the outset of a client relationship and on an ongoing basis thereafter. Screening should cover clients, beneficial owners, directors, and other relevant parties, and should be performed against up-to-date sanctions lists and any applicable local or international designations. Where a commercial screening database is used, it should be properly configured to reflect the firm's risk profile, with clear processes in place for reviewing and resolving potential matches. Screening should also be repeated periodically and whenever there are changes in client circumstances to ensure continued compliance.

7.51 Where a commercial database is not available, firms should carry out manual screening by consulting official sanctions lists published by the FSIU (https://www.gov.bm/international-sanctions-measures) . This may include searching names (and known aliases) directly against publicly available lists and verifying identifying details such as date of birth, nationality, and address to distinguish between true and false matches. While manual screening can be effective, it requires particular care to ensure consistency, completeness, and timeliness.

7.52 In all cases, it is essential that firms fully document the screening process. Records should include the date of the search, the sources used, the names screened, the results obtained, and any steps taken to resolve potential matches. Proper documentation provides an audit trail, supports decision-making, and demonstrates compliance with financial sanctions obligations.

7.53 Firms should report immediately any matches on the sanctions list. The FSIU CRF process requires firms to: (i) report immediately upon identifying a match with a designated person on the UK Consolidated List or other applicable sanctions list; (ii) report immediately upon suspecting that a sanctions obligation has been or is about to be breached or evaded; (iii) provide full details of the designated person, the nature of the funds or economic resources involved, and the action taken; and (iv) freeze without delay any funds or economic resources and await further instruction from the FSIU.

7.54 The CRF for targeted financial sanctions should be used to submit all relevant compliance information to the FSIU of the Ministry of Legal Affairs. This includes reporting suspected designated persons (Part B), details of assets that have been frozen (Part C), and any suspected breaches of financial sanctions (Part D). Users should ensure that all information provided is accurate and complete to the best of their knowledge, as the submission may be shared by the Ministry of Legal Affairsto support compliance with sanctions regulations. Supporting annexes included with the form provide definitions and guidance to assist completion, and reference should also be made to the FSIU's general guidance, which outlines applicable legal obligations, including circumstances where reporting is mandatory and failure to do so may constitute a criminal offence. Completed forms, along with any supporting documentation, must be submitted to the FSIU via email or post in accordance with the stated instructions, and independent legal advice should be sought

where there is any uncertainty regarding reporting or compliance obligations. The CRF and related instructions can be found at:

https://www.gov.bm/sites/default/files/FSIU_Compliance_Reporting_Form_June_2022.pdf

7.55 RPFs should ensure that their Reporting Officers and relevant staff are familiar with the CRF process and that it is integrated into the firm's internal reporting procedures alongside the SAR process.

Persons firms should not accept as clients

7.56 Recommendation 6 and 7[15] of the FATF Standards require that countries implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions ("UNSCRs") relating to the prevention and suppression of terrorism and terrorist financing, and the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

Prevention and suppression of terrorism and terrorist financing

7.57 In 2011, Bermuda implemented measures to strengthen its approach to combating terrorism and preventing the financing of terrorist activities. These measures ensure that effective systems are in place to identify and freeze assets linked to terrorism and to restrict activities that could support such acts. The overall objective is to prevent and disrupt the funding and facilitation of terrorism. To achieve this, a set of core prohibitions has been established, and failure to comply with these restrictions may result in criminal penalties:

i. dealing with the funds and economic resources of a designated person;

ii. making funds or financial services available to a designated person;

iii. making funds or financial services available for the benefit of a designated person;

iv. making economic resources available to a designated person; and

[15] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of the FATF Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Recommendation, (February 2012), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010).

The requirements of UNSC Resolution 1373 (2001) were previously implemented in Bermuda through the Terrorism United Nations Measures) (Overseas Territories) Order 2001 (“2001 Order”) and the Terrorist Asset- Freezing (Temporary Provisions) Act 2010.

v. making economic resources available for the benefit of a designated person.

7.58 RPFs must ensure they are aware of and compliant with all applicable sanctions regimes as updated from time to time. These restrictive measures include, inter alia, an arms embargo, asset freezing measures and the prohibition on the provision of assistance to persons and entities designated by the United Nations Security Council or European Union as associated with ISIL (Da'esh) or Al-Qaida. The Afghanistan Order 2012 places restrictive measures on certain persons and entities associated with the Taliban. These restrictive measures include, inter alia, asset freezing measures and the prohibition of the supply of military goods and technical assistance related to military activities to designated persons.

Prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing

7.59 Sanctions relating to the Democratic People's Republic of Korea (DPRK) are in force in Bermuda to give effect to international measures aimed at restricting activities that could support weapons development and military programmes. These measures prohibit the direct or indirect sale, supply, or transfer of arms and related materials, as well as goods, technology, and items that could contribute to nuclear, ballistic missile, or other weapons programmes. Restrictions also apply to certain dual-use goods and luxury items, along with limitations on providing technical assistance, training, financial services, or other forms of support to the DPRK.

7.60 Similarly, sanctions measures relating to Iran are implemented in Bermuda to reflect international efforts to address concerns regarding nuclear proliferation and related activities. These measures include the freezing of funds and economic resources belonging to designated individuals and entities, as well as restrictions on trade in specified goods and materials. Together, these controls are intended to limit access to financial systems and resources that could be used to support prohibited activities.

7.61 The FSIU Bermuda CPF Guidance (May 2025) provides detailed guidance on PF risks, including DPRK and Iran evasion typologies, indicators, and reporting obligations. The FATF's June 2025 report on complex proliferation financing and sanctions evasion schemes identified emerging typologies including:

i. use of virtual assets and digital platforms to evade sanctions;

ii. sophisticated trade-based schemes involving falsified documentation;

iii. exploitation of jurisdictions with weak AML/CFT/CPF frameworks as transit points; and

iv. use of professional intermediaries (including accountants) to create layers of corporate structures designed to obscure sanctioned ownership.

RPFs must incorporate these typologies into their training and monitoring programmes.

7.62 It should be appreciated that any obligations that arise under the Orders are in addition to any obligations under the Relevant Legislation and are separate from those obligations. The full text of the Orders are available at: www.legislation.gov.uk and the International Sanctions Act Regulations are available at: www.bermudalaws.bm. Firms should ensure that they fully understand their obligations under this legislation. As appropriate, firms should take legal advice to assist in their understanding and compliance.

7.63 The links provided below may be of assistance in relation to financial sanctions regimes in the United Kingdom, the European Union, the United States and United Kingdom:

Office of Financial Sanctions Implementation HM Treasury: Office of Financial Sanctions Implementation **European Union - External Relations:** Common Foreign & Security Policy (CFSP) - Sanctions or restrictive measures in force: http://eeas.europa.eu/archives/docs/cfsp/sanctions/docs/measures_en.pdf

United States of America -- Office of Foreign Asset Control: U.S. Treasury - Office of Foreign Assets Control:

https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-ForeignAssets-Control.aspx

CHAPTER 8: OUTSOURCING

Regulation 14

Regulation 14A

Regulation 15

Reliance

8.1 Pursuant to Regulation 14, a firm may rely on certain third parties to perform CDD measures provided that both the third party and the nature of the reliance meet certain criteria. In any reliance situation, however, the relying firm retains responsibility for any failure to comply with a requirement of the Regulations as this responsibility cannot be delegated.

8.2 Firms should utilise a risk-based approach when determining the level of reliance that can be placed on the third party and the verification work the third party has carried out, and as a consequence, the amount of evidence that should be obtained directly from the customer.

8.3 Part of the firm's AML/ATF/CPF policy statement should address the circumstances where reliance may be placed on other entities and how the firm will assess whether the other entity is regulated for AML/ATF/CPF purposes.

8.4 The CDD measures that a firm may rely upon a third party to apply are:

i. identifying the customer and verifying the customer's identity;

ii. identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner; and

iii. understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

8.5 In any reliance situation, the following duties remain with the relying firm and cannot be delegated:

i. the duty to conduct on-going monitoring to scrutinise transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the firm's knowledge of: (i) the customer; (ii) beneficial owner; (iii) purpose and intended nature of the business relationship; and (iv) where necessary, the source of funds or wealth; and

ii. the duty to report knowledge or suspicion of money laundering or terrorist financing.

8.6 A firm may rely upon a third party who is:

i. for Bermuda persons:

(a) an AML/ATF/CPF regulated financial institution under section 42A(1) of POCA; or

(b) an independent professional as defined at Regulation 2(1);

ii. for non-Bermuda persons:

(a) a person who carries on business in a country or territory other than Bermuda who is an institution that carries on business corresponding to the business of an AML/ATF/CPF regulated financial institution; or

(b) an independent professional subject to equivalent mandatory professional registration and supervision.

8.7 Firms must enter into a reliance agreement with the third party. The agreement should specify that the firm intends to rely upon the third-party institution for the purposes of Regulation 14(1)(a) and that the third party consents to such reliance. This consent must confirm that, upon request by the relying firm, the third party will make available, the firm's copies of the verification data and other relevant documents or information on the customer, beneficial owner, and purpose and intended nature of the business relationship that the third party obtained when applying CDD measures.

Basis of reliance

8.8 Firms must not rely upon any third party or enter into agency or correspondent arrangements where access to verification data without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions.

8.9 Firms should also consider any geographic AML/ATF/CPF risks associated with the country or territory in which the third party is based and the degree to which the third party has effective measures in place to mitigate such risks. When the intermediary is located in a higher-risk jurisdiction, the business should not proceed unless the identity of the underlying customer and each beneficial owner has been verified to the satisfaction of the firm.

8.10 For reliance to be permissible, the relying firm should obtain certain information immediately, including:

i. the identity of the customer;

ii. the identity of the beneficial owner;

iii. the purpose and intended nature of the business relationship; and

iv. the level of CDD that has been carried out.

8.11 Firms may also only rely on verification actually carried out by the entity being relied upon. An entity that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another entity.

8.12 Whether an entity wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's status may include consideration of matters such as:

- its public disciplinary record, to the extent that this is available;
- the nature of the client the service sought and the sums involved;
- any adverse experience of the other entity's general efficiency in business dealings; and
- any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the entity to be relied upon.

8.13 Reliance on a third party to apply certain CDD measures cannot be absolute. For a firm to rely upon the verifications carried out by a third party, the verification that the third party has carried out must have been based upon at least the standard level of customer verification. With the exception of situations in which an underlying customer is confirmed as falling under Regulations 10(2), 10(3), 10(4) or 10(5), it is not permissible to rely upon simplified due diligence carried out.

Group Introductions

8.14 Where customers are introduced between different parts of the same group, entities that are part of the group may rely upon the identification and verification procedures conducted by that part of the group which first dealt with the customer, provided the following criteria are met:

i. the group entity that carried out the CDD measures can be relied upon as a third party under this guidance;
ii. the group has implemented a group-wide AML/ATF programme;
iii. the group entity makes available to the group the information described paragraph 8.6;
iv. foreign branches and majority owned subsidiaries of the group apply AML/ATF measures that are consistent with the group's home country AML/ATF requirements;
v. the customer's relationship with the relying firm requires an equal or lower level of CDD measures as compared to those actually applied by the relied upon institution;
vi. the group's home is in Bermuda or in a jurisdiction that imposes equivalent AML/ATF requirements; and

vii. a reliance agreement is in place between the firm and the group entity being relied upon.

In such cases, one member of a group may confirm to another member of the group that the identity of the customer has been satisfactorily verified.

8.15 Where Bermuda firms have day-to-day access to all group client information and records, there is no need to obtain a group introduction confirmation, if the identity of that client has been verified previously to AML/ATF/CPF standards in Bermuda, or in an equivalent jurisdiction. However, if the identity of the client has not previously been verified, for example because the group client relationship pre-dates the introduction of regulations, or if the verification evidence is inadequate, any missing verification evidence will need to be obtained.

Regulation 15(6)

8.16 An entity which carries on business in Bermuda and is relied on by another person to apply CDD measures must, within the period of five years beginning on the date on which it is relied on, if requested by the firm relying on it, as soon as reasonably practicable, make available any relevant copies of any identification and verification data and other relevant documents on the identity of the client which the third party obtained when applying customer due diligence measures.

8.17 A firm must document the steps taken to confirm that the entity relied upon is a relevant person satisfies the requirements in Regulation 14(2). This is particularly important where the entity relied upon is situated in a country or territory other than Bermuda.

Regulation 15(7)

8.18 A firm which relies on an entity situated in a country or territory other than Bermuda to apply CDD measures must take steps to ensure that the entity on which it relies will, within the period of five years beginning on the date on which the third party is relied on, if requested, comply with the obligations to retain and maintain information as set out above.

Situations which are not reliance: One firm or entity acting solely as introducer

8.19 When a third party acts solely as an introducer between a customer and a firm and the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, all identification and verification obligations lie with the firm providing the service. This does not preclude the introducing entity from carrying out identification and verification of the customer on behalf of the firm providing the service, if the introducer is an agent for that firm.

Third party as agent of the firm

8.20 Where the third party is an agent or appointed representative of the firm, it is an extension of that firm. In such cases, the third party agent may obtain the appropriate verification evidence in respect of the customer, but the firm providing the service is responsible for

first specifying what should be obtained, and for ensuring that records of the verification evidence taken in respect of the customer are appropriately retained and accessible.

Outsourcing

8.21 Outsourcing is an arrangement in which a firm uses a third-party (the outsourcing service provider) to perform activities such as applying CDD measures on an ongoing basis that would otherwise be undertaken by that firm.

8.22 Outsourced activities should be carried out in accordance with the firm's policies, and the firm should have effective control over the service provider's implementation of those policies. A firm's board or similarly empowered body or individual, such as the Compliance Officer, should establish clear accountability for all outsourced activities, as if the activities were performed in-house according to the firm's own standards of internal control and oversight.

8.23 In any outsourcing arrangement, a firm cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML/TF/PF.

8.24 Regulation14A provides that where a firm delegates its AML/ATF/CPF compliance function to a service provider, the firm must retain ultimate responsibility for the AML/ATF/CPF compliance function. Ultimate responsibility includes the obligation to:

i. ensure that the service provider has in place AML/ATF/CPF systems controls and procedures that are in compliance with the Bermuda AML/ATF/CPF requirements and are subject to the Regulations and these Guidance Notes;

ii. consider and assess the effect the outsourcing compliance functions has on the ML/TF/PF risk and record such assessment; and

iii. monitor any perceived risk on an ongoing basis to ensure that the roles, responsibilities and respective duties are clearly defined, documented and understood.

8.25 In any outsourcing relationship, the firm should take care to avoid:

i. impeding the effective ability of the firm's senior management to monitor and manage the firm's compliance functions, including the application of non-standard measures, such as enhanced due diligence;

ii. impeding the effective ability of the firm's board or similarly empowered body or individual to provide oversight;

iii. impeding the effective ability of the Board to monitor the firm's compliance with all obligations under the regulatory system;

iv. reducing the responsibility of the Bermuda RFI and/or its managers and officers;

v. removing or modifying any conditions subject to which the firm's authorisation was granted; and

vi. increasing ML/TF/PF risk in any way that is not adequately addressed through appropriate risk assessment and mitigation.

8.26 In any outsourcing relationship the firm should retain in-house the resources and expertise necessary to:

i. set the firm's risk policies and procedures;

ii. continuously identify, assess, monitor and manage the risks associated with outsourcing activities to the service provider;

iii. continuously supervise, monitor and test the adequacy of the activities carried out by the service provider; and

iv. ensure the firm's ability to resume direct control over the outsourced activity in the event that a need arises.

8.27 Both prior to entering into and throughout any outsourcing arrangement, a firm should identify and assess the risks created by outsourcing the proposed activities. In particular, a firm should assess whether and how outsourcing may affect its ability to fulfil its obligations under the Regulations and these Guidance Notes. Where all risks identified and assessed can be effectively and appropriately mitigated, those risks should be mitigated. Where all risks identified and assessed cannot be effectively mitigated, a firm should not enter into the outsourcing arrangement.

8.28 Firms considering an outsourcing arrangement should carry out due diligence as to the service provider under consideration. The purpose of the due diligence is to determine whether the service provider has the ability, capacity, and any required authorisation to perform the outsourced activities reliably, professionally, and in accordance with the Regulations and these Guidance Notes. Firms should establish a written policy concerning the scope and frequency of initial and on-going due diligence carried out as to such service providers.

8.29 In determining whether the use of a service provider outside of Bermuda is appropriate, firms should conduct enhanced due diligence to evaluate their ability to effectively monitor the foreign service provider, maintain the confidentiality of firm and client information, and execute contingency plans and exit strategies.

8.30 At a minimum the firm should conduct due diligence with respect to a service provider and consider the following;

i. whether the service provider is a licensed provider;

ii. whether the service provider is effectively regulated for AML/ATF/CPF purposes;

iii. any operational, financial, human resource, structural, legal or regulatory considerations may affect the service provider's ability to carry out the

outsources activities or impede the firm's ability to access relevant information;

iv. whether the service provider has an effective contingency plan in event of operational, financial, human resources, structural, legal or regulatory considerations that negatively impact the service providers ability to carry out the outsourced activities;

v. whether any confidential, secrecy, privacy or data protection restrictions may impede the firm's ability from effectively monitoring the activities of the service provider;

vi. whether the service provider can maintain the confidentially of the firm and its client information; and

vii. whether the service provider has effective procedures in place to back up and protect the data of the firm in the event of a cyber breach or other disasters.

8.31 The firm must execute with the service provider a comprehensive, written and legally binding agreement governing the outsourcing arrangement (Agreement). This should be governed by Bermuda Law; and if not, then the agreement should be governed by the laws of a jurisdiction that imposes equivalent AML/ATF/CPF requirements.

8.32 The Agreement should:

i. include a clear statement of functions to be outsourced;

ii. precisely define the rights and obligations of the firm and the service provider;

iii. specify all activities being outsourced;

iv. clearly state all requirements, including regulatory obligations, concerning the service provider’s performance of the outsourced activities;

v. specify the persons at both the firm and the service provider who are responsible for implementing, monitoring, and managing the outsourcing arrangement;

vi. specifically state the name or title of the RFI’s Bermuda officer who retains ultimate responsibility for the RFI’s compliance with the Regulations and these Guidance Notes;

vii. establish qualitative and quantitative performance standards to enable the firm to assess the adequacy of service provision and authorise and require the firm to continuously monitor and assess the service provider against the established performance standards in order to ensure that any necessary corrective measures are taken promptly;

viii. oblige the service provider to allow the firm’s specified persons complete, constant, and unfettered access to all data relating to the outsourced activity;

ix. require the service provider to maintain appropriate procedures to back up and ensure the protection of confidential information;

x. expressly permit the firm to take remedial action where the service provider's performance falls short of that required by the Agreement, the Regulations, or these Guidance Notes or where the Board orders the firm in writing to do so;

xi. entitle the firm to terminate the outsourcing arrangement where the service provider undergoes a change of control, becomes insolvent, goes into liquidation or receivership, or for any reason materially fails to perform according to the outsourcing agreement, the Regulations, and these Guidance Notes;

xii. require the firm and the service provider to establish, implement, and maintain a contingency plan for disaster recovery and for periodic testing of backup facilities;

xiii. include a termination and exit management clause that allows the outsourced activities and any related data to be transferred to another service provider or to be reincorporated into the outsourcing firm.

Subcontracting

8.33 Any subcontracting arrangement should be detailed in the outsourcing agreement. If the outsourcing agreement allows the service provider to subcontract any of the activities to be outsourced, any subcontractor should be subject to the same levels of due diligence as the primary service provider. Additionally, any subcontractor should be required to adhere to all aspects of the outsourcing agreement and to the outsourcing firm's responsibilities under the Regulations and these Guidance Notes. The outsourcing firm should be required to approve in writing any changes to the subcontracting arrangements.

CHAPTER 9: TRAINING

Regulation 18

9.1 Regulation 18 requires a relevant person to take appropriate measures so that all relevant employees are made aware of the laws relating to money laundering, terrorist and proliferation financing and regularly given training in how to recognize and deal with transaction which may be related to money laundering, terrorist or proliferation financing. The effective application of even the best designed control systems can be quickly compromised if staff lack competence or probity, are unaware of or fail to apply systems and controls and are not adequately trained.

9.2 Regulation 18(2) defines a relevant employee as an employee who at any time in the course of his duties has or may have access to any information which may be relevant in determining whether any person is engaged in money laundering, terrorist or proliferation financing. For the purposes of Regulation 18, "relevant employee" includes an individual working on a temporary basis whether under a contract of employment, contract for services or otherwise.

9.3 One of the most important controls over the prevention and detection of money laundering, terrorist and proliferation financing is to have appropriately vetted staff who are: (i) alert to money laundering, terrorist and proliferation financing risks; and (ii) well trained in the identification of unusual or higher risk activities or transactions, which may indicate money laundering, terrorist or proliferation financing activity.

9.4 Therefore all relevant employees will need to have a basic understanding of money laundering, terrorist and proliferation financing and an awareness of internal reporting procedures (including the identity of the Reporting Officer and the statutory penalties for noncompliance). It is important for senior management to make employees aware of their obligations and to provide regular training on how to discharge them.

9.5 A firm must have appropriate measures in place to make relevant employees aware of:

i. the firm's business systems and controls (including policies and procedures) designed to prevent and detect money laundering, terrorist and proliferation financing;

ii. the statutory obligations under which the business operates and under which employees may be held personally liable; and

iii. the implications of failing to report information in accordance with procedures, and that as well as criminal, civil or regulatory sanctions, disciplinary proceedings can also rise.

9.6 A firm may demonstrate that it has appropriate measures in place where it:

i. provides relevant employees with a copy of, or intranet access to, the firm's procedure manual for AML/ATF/CPF/Sanctions;

ii. informs staff of the identity of the Reporting Officer and the procedures to make internal SARs;

iii. provides relevant employees with a document outlining the firm's and their own obligations and potential criminal liability under the AML/ATF/CPF legislation and this Guidance;

iv. requires employees to acknowledge that they have received and understood the business' procedures manual and document outlining statutory obligations; and

v. periodically tests employees' awareness of policies and procedures and statutory obligations.

9.7 It is not sufficient solely to provide employees with a copy of these Guidance Notes as these are designed to provide a base from which a firm can design and implement systems and tailor its own policies and procedures appropriate to its business.

9.8 A firm may demonstrate that it has appropriate measures to maintain awareness where it:

i. keeps employees aware of money laundering, terrorist and proliferation financing developments (such as updates issued by the Board or the Office of the Office of the National Anti-Money Laundering Committee ("NAMLC"), or developments in international standards) as they occur;

ii. provides employees with case studies illustrating how products or services provided by the financial services business may be abused;

iii. advises employees of current news stories involving money laundering, terrorist and proliferation financing activity and sanctions; and

iv. sends e-mail reminders of employee obligations and the need to remain vigilant.

9.9 The guiding principle of all anti-money laundering, terrorist and proliferation financing training should be to encourage employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the business against the threat of money laundering, terrorist and proliferation financing. A firm may demonstrate the provision of adequate training where the training promotes an awareness of the threat of money laundering, terrorist and proliferation financing and the reporting procedures that should be followed in the event that unexplained unusual, or higher risk activity or transactions are spotted.

Training must:

i. be tailored to the business and relevant to the employees to whom it is delivered;

ii. highlight to employees the importance of the contribution that they can individually make to the prevention and detection of money laundering, terrorist and proliferation financing; and

iii. cover key aspects of legislation to prevent and detect money laundering, terrorist and proliferation financing.

9.10 A firm may demonstrate the provision of adequate training to relevant employees where it addresses:

i. the acts, regulations and guidance notes relating to money laundering, terrorist and proliferation financing legislation and sanctions;

ii. the acts, regulations and guidance notes relating to PEP's

iii. vulnerabilities of services and products offered by the firm, and subsequent money laundering, terrorist and proliferation financing risk;

iv. policies and procedures, and employees' responsibilities;

v. application of risk based CDD policies and procedures;

vi. recognition of and dealing with unusual or higher risk activity and transactions, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships;

vii. money laundering, terrorist and proliferation financing developments, including techniques, methods, trends and typologies; and

viii. management of client relationships which have been the subject of a SAR, e.g. risk of committing the offence of tipping-off, and dealing with questions from such clients, and/or their advisers.

9.11 A firm may demonstrate the provision of adequate training where (in addition to training for relevant employees) it addresses:

i. the design and implementation of systems and controls to counter money laundering, terrorist and proliferation financing;

ii. the design and implementation of compliance testing and monitoring programs;

ii. the handling and validation of internal disclosures;

iv. liaising with the FIA and law enforcement;

v. management of the risk of tipping-off; and

vi. the handling of, for example, production and restraint orders.

9.12 A firm may demonstrate the provision of training at appropriate frequencies by:

i. providing all employees with induction training within 30 days of the commencement of employment and, when necessary, where there is a subsequent change in an employee's role; and

ii. delivering training to all employees at least annually and otherwise determining the frequency of training for relevant employees based on risk, with more frequent training where appropriate.

9.13 A firm may demonstrate that it has assessed the effectiveness of training provided by:

i. testing employee's understanding of the business' policies and procedures to combat money laundering, terrorist and proliferation financing, and their ability to recognize money laundering, terrorist and proliferation financing activity;

ii. monitoring the compliance of employees with systems and controls (including policies and procedures) to prevent and detect money laundering, terrorist and proliferation financing, and taking any action that may be necessary;

iii. monitoring internal reporting patterns, and taking any action that may be necessary; and

iv. the routine supervision of employees.

PF and Sanctions Training Requirements

9.14 Training programs must be updated to include the following CPF and sanctions-related content:

i. the nature of proliferation financing risks and their relevance to the accounting sector, including the definition of PF as the potential breach, non-implementation or evasion of targeted financial sanctions obligations as referred to in the Regulations;

ii. sanctions obligations under the International Sanctions Act 2003, International Sanctions Regulations 2013, and all applicable sanctions Orders in Council, including the obligation to freeze without delay funds and economic resources belonging to or controlled by designated persons should be included in the training;

iii. sanctions screening procedures, including the use of the HM Treasury Consolidated List and the firm's screening systems, the frequency of screening, and the process for handling potential matches and false positives;

iv. PF risk indicators as set out in the FSIU Bermuda CPF Guidance (May 2025), including customer indicators, transaction indicators, trade-based indicators, and country and geographic indicators;

v. the distinction between SAR reporting to the FIA via the goAML electronic platform and CRF reporting to the FSIU, including the dual reporting obligation that arises where a suspicion relates to both potential money laundering, terrorist and proliferation financing and a potential breach of sanctions;

vi. asset-freezing obligations and the prohibition on making funds or economic resources available to designated persons, including the requirement to report immediately to the FSIU and the consequences of non-compliance; and

vii. relevant training events, including NAMLC and CFATF training sessions such as the February 2026 CFATF-led training on revised FATF Standards held in Bermuda.

9.15 Training must be provided to all relevant staff on commencement of employment and at regular intervals thereafter. Records of training provided, including the date, content covered, attendees and results of employee tests, must be maintained in accordance with the record-keeping requirements set out in Chapter 10 of these Guidance Notes.

9.16 A firm must keep adequate and orderly records for five years detailing the dates on which training on the prevention and detection of money laundering, terrorist and proliferation financing was provided, the nature of the training and the names of employees who received the training.

CHAPTER 10: RECORD KEEPING

Regulation 15

10.1 The record keeping obligations of the Regulations and additional regulatory requirements are essential to facilitate effective investigation, prosecution and confiscation of criminal property. If law enforcement agencies, either in Bermuda or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for money laundering, terrorist and proliferation financing and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity cannot be traced back through the financial system, then the sources and the destination of terrorist funding will not be identified.

10.2 Regulation 15 provides for record keeping procedures to be followed by a relevant person. Records may be kept:

i. by way of original documents;

ii. by way of photocopies of original documents (certified where appropriate);

iii. microfiche, electronic storage, hard drive

iv. in scanned form; or

v. in computerized or electronic form.

10.3 Regulation 15(2) requires the following records to be kept:

i. a copy of or the references to, the evidence of the client's identity obtained pursuant to Regulations 6, 8B(7), 11, 13(4) or 14; and

ii. the supporting evidence and records (consisting of the original documents or copies admissible in court proceedings) in respect of the business relationships and occasional transactions which are the subject of client due diligence.

10.4 Regulation 15(3) requires a relevant person to retain records in relation to evidence of identity for at least five years beginning on the date on which the business relationship ends, or in the case of an occasional transaction five years beginning on the date on which the transaction is completed. Regulation 2 defines an independent professional as a Relevant Person for the purposes of the records retention requirements.

10.5 A firm must ensure that the way in which CDD information is recorded and stored facilitates periodic updating of the information. A firm may demonstrate adequate recording and storage of CDD information by ensuring that updated information relating to a client that is obtained through meetings, discussions, or other methods of communication with the client is recorded and retained. Records must contain the following details of each transaction carried out with or for a client during business activities specified by Regulation 2:

i. name and address of the client;

ii. if a monetary transaction, the kind of currency and the amount;

iii. if the transaction involves a client's account, the number, name or other identifier for the account;

iv. date of the transaction;

v. details of the counterparty, including account details;

vi. nature of the transaction; and

vii. details of the transaction.

10.6 The records prepared and retained by a firm in relation to client transactions and activity must be orderly and such that the audit trail for incoming and outgoing funds or asset movement is clear and complete. Adequate recording of details of transactions may be demonstrated by recording all transactions undertaken on behalf of a client within that client's records, enabling a complete transaction history for each client to be easily constructed.

10.7 Adequate recording of details of transactions may be demonstrated by including (where appropriate):

i. valuation(s) and price(s);

ii. the form (e.g. cash, cheque, electronic transfer) in which funds are transferred;

iii. memoranda of instruction(s) and authority(ies);

iv. memoranda of purchase and sale;

v. custody of title documentation; and

vi. other records in support of transaction of records where these are necessary to enable a clear and complete audit trail of fund or asset movements to be established.

10.8 A firm must keep for at least five years adequate and orderly records to enable the Board, internal and external auditors and other competent authorities to assess the effectiveness of systems and controls that are maintained by a firm to prevent and detect money laundering, terrorist and proliferation financing.

10.9 A firm must keep adequate and orderly records documenting its policies and procedures to prevent and detect money laundering, terrorist and proliferation financing for at least five years from the date those policies and procedures are superseded.

10.10 A firm may demonstrate that it has retained adequate records where it keeps:

i. its risk assessment;

ii. compliance reports to senior management; and

iii. the working papers to the extent that these provide details of the testing programs conducted.

This does not necessitate the retention of all compliance testing working papers.

10.11 A firm must keep, for a period of five years from the date a business relationship ends, or, if in relation to an occasional transaction, for five years from the date that a transaction was completed, orderly records containing:

i. internal SARs and supporting documentation;

ii. the decision of the Reporting Officer concerning whether to make an external SAR and the basis of that decision; and

iii. any external SARs in relation to that business relationship or an occasional transaction.

10.12 A firm must keep adequate and orderly records containing the findings of reviews of:

i. complex transactions;

ii. unusual large transactions; and

iii. unusual patterns of transactions which have no apparent economic or visible lawful purpose, for a period of five years from the date the business relationship ends, or, if in relation to an occasional transaction, for five years from the date that the transaction was completed.

10.13 A firm must keep adequate and orderly records containing the findings of review of clients and transactions:

i. connected with jurisdictions which do not or insufficiently apply the FATF Recommendations, where the business relationship or transaction has no apparent economic or visible lawful purpose; or

ii. which is the subject of international countermeasures for a period of five years from the date the business relationship ends, or, if in relation to a one-off transaction, for five years from the date that the transaction was completed.

10.14 A firm must ensure that the way in which CDD information (including transaction information) is recorded facilitates ongoing monitoring of each relationship.

10.15 For all other purposes, the records retained by a firm must be readily accessible by the firm. A firm must periodically review the accessibility of, and condition of, paper and electronically retrievable records and ensure adequate consideration of the safekeeping of records.

10.16 A firm must periodically test procedures relating to retrieval of records.

10.17 A firm that undergoes mergers, take-overs, or internal reorganizations, must ensure that records remain readily retrievable for the required period when rationalizing computer systems and storage arrangements.

10.18 Records must be maintained in a format which would enable the firm to respond fully and rapidly to enquiries received from the FIA or law enforcement relating to:

i. whether it maintains, or has maintained during the previous five years a business relationship with any person and;

ii. the nature of that relationship.

10.19 Where documentation is held overseas or by third parties, such as under outsourcing arrangements, or where reliance is placed on introducers or intermediaries, this will present additional factors for a firm to consider. Where record keeping is outsourced, a firm remains responsible for compliance with all requirements.

10.20 Where an introducer ceases to trade or have a relationship with a client that it has introduced a firm, particular care needs to be taken to retain, or hand over, the appropriate client records.

10.21 A firm must not enter outsourcing arrangement or place reliance on third parties to retain records where access to records is likely to be impeded by confidentiality or data protection restrictions.

10.22 Record keeping arrangements must be agreed with the Board where a firm terminates activities or disposes of business or a block of client relationships to another accounting firm or service provider. Where a firm terminates activities or disposes of business or a block of client relationships to other Firms or service providers, record keeping requirements are unaffected by the termination or disposal.

PF and Sanctions Record Keeping

10.23 In addition to the records specified above, firms must maintain the following records relating to proliferation financing and sanctions compliance:

i. PF risk assessments and any updates thereto, including the methodology used and the conclusions reached, and evidence that the risk assessment has been reviewed and approved by senior management;

ii. sanctions screening results for all clients and beneficial owners, including the date of screening, the lists screened against, the outcome, and the records of any false positive resolutions;

iii. FSIU, including records of any asset-freezing actions taken;

iv. records of any assets frozen or reports made under sanctions regimes, including the designated person's details, the nature and value of frozen assets, the date of freezing, and any licenses obtained from the Governor or relevant authority; and

v. records of any decisions not to proceed with a transaction or business relationship on sanctions grounds, including the reasons for the decision and the date on which it was taken.

10.24 All records relating to proliferation financing and sanctions compliance must be retained for a minimum of five years from the date on which the relevant business relationship or transaction was completed, in accordance with the retention periods set out in the Regulations. Records must be maintained in a form that allows them to be made available to the Board, the FIA, or the FSIU promptly upon request.

CHAPTER 11: INTERNAL AUDIT

Independent audit function[16]

11.1 An accountancy firm engaging in specified activities pursuant to section 49(5) of POCA must provide an independent audit on registration pursuant to Regulation 17A. Per Regulation 17A(1) the audit must "*be conducted by a qualified independent third party or internally by persons independent of any other function, the lines of business over which the function has audit responsibilities, and financial operations*."

11.2 The Board may consider an auditor qualified if they have the requisite subject matter expertise and proficiency to competently review the firm's AML/ATF/CPF policies, procedures, and controls. Such expertise and proficiency may be evidenced by continuing training and professional education focused on AML/ATF/CPF, including internationally recognized certifications. Proof of the relevant qualifications and independence of the auditor shall be submitted with the independent audit on registration.

11.3 Any person who is involved in establishing or performing any of the firm's ongoing AML/ATF/CPF compliance processes should not conduct an audit, determine the scope of an audit, or have the authority to alter the contents of an audit report before its delivery to senior management and the firm's governing body. A firm that seeks to use in-house employees to conduct an AML/ATF/CPF independent audit should evaluate the reporting lines of the audit employees and verify their independence when reporting audit results.

11.4 Per Regulation 17A(2), "*the independent audit function must provide and document an independent and objective evaluation of the robustness of the firm's AML/ATF framework, and the reliability, integrity, and completeness of the design and effectiveness of the AML/ATF risk management function and AML/ATF internal controls framework, and the AML/ATF compliance."*

As such the Board requires the audit function to provide for a documented audit of the firm's AML/ATF/CPF policies, procedures and controls, including those policies, procedures and controls relating to compliance with international sanctions. The audit must sample test the implementation, integrity and effectiveness of their AML/ATF/CPF policies, procedures, and controls. The audit should be conducted more frequently when senior management becomes aware of any gap or weakness in the AML/ATF/CPF policies, procedures or controls or when senior management deems it necessary due to the Firm's assessment of the risks it faces.

[16] Bermuda Monetary Authority, Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF August 2022; Independent Audit – section 1.78 – 1.83

11.5 For clarity, the audit function must, at a minimum[17]:

a) assess the reliability, integrity and completeness of the firm's AML/ATF/CPF policies, procedures and controls, including with respect to:

i. risk assessment adequacy;

ii. risk mitigation and other measures to manage higher risks;

iii. CDD;

iv. ongoing monitoring;

v. detecting and reporting knowledge, suspicion and reasonable grounds for suspicion of ML/TF/PF;

vi. international sanctions;

vii. Record-keeping and retention;

viii. Reliance and outsourcing relationships;

ix. testing of the risk-based approach; and

x. the National Risk Assessment considerations.

b) evaluate the firm's risk assessment processes and the risk ratings the firm has assigned with respect to its size, customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions (risk-based approach);

c) test compliance with the relevant laws and regulations;

d) test the AML/ATF/CPF controls for the firm's transactions and activities, with an emphasis on higher risk areas;

e) test CDD, that should include a clear representation of the firm's clients that include High, Medium and Low-rated clients; noting that the sampling should be risk-based, with appropriate emphasis on higher-risk clients as per the Firm's risk assessment;[18]

f) assess employees' knowledge of the relevant Bermuda acts, regulations and guidance, the firm's policies, procedures and controls and the role of each relevant employee within the firm;

g) assess the adequacy, accuracy and completeness of employee training and awareness programmes; and

h) review the firm's past audit reports to assess the efficacy with which the firm has implemented previously recommended changes and the timeliness of completion.

[17] The Independent Audit report must report on all areas noted herein

[18] The Board expects the independent audit to contain evidence of file testing (which may be anonymized) that can be verified by the Board if deemed necessary.

11.6 Firms should note that the results of the independent audit may be considered as part of the supervisory engagement for the desktop and onsite reviews - as such it is important that the results are truly independent from senior management. [19]

11.7 Firms should note the Board **will not** accept an independent audit that:

i. is not sufficiently detailed;

ii. is conducted by a person without relevant expertise;

iii. is conducted by a person who is not sufficiently independent; or

iv. is not completed within six months of the registration date by the firm.

CPF and Sanctions Audit Requirements

11.8 The annual independent audit must additionally cover the following areas:

i. CPF framework (AML/ATF) - the audit must assess whether the firm has integrated CPF into its existing AML/ATF systems and controls as required;

ii. sanctions compliance program effectiveness - the audit must assess whether the firm's sanctions screening, reporting, and asset-freezing procedures are operating effectively;

iii. screening system adequacy - the audit must assess whether the firm's sanctions screening tools and processes are adequate to identify matches with the HM Treasury Consolidated List and other applicable lists;

iv. PF risk assessment adequacy - the audit must assess whether the firm's PF risk assessment is comprehensive, current, and approved by senior management; and

v. Per AML/ATF Board 2025/2026 requirement: the independent audit must be completed within 6 months of the firm's registration date (October 31 of each year for most firms). Audits that are not sufficiently detailed or are not completed within this timeframe will not be accepted by the Board.

11.9 The Board expects that auditors conducting the independent audit will have appropriate qualifications and experience in AML/ATF/CPF compliance and sanctions compliance. The audit report must be provided to the Board upon request and must include detailed findings, specific recommendations, and documented management responses. Firms must maintain evidence that any deficiencies identified in the audit have been remediated and addressed within a reasonable timeframe and must inform the Board of any material deficiencies that remain unresolved.

[19] NOTE: Please ensure that all submitted documents are in **machine-readable PDF** or editable document formats (i.e.: Word, Excel or searchable PDF's). Scanned or image-based PDFs must be accompanied by OCR (Optical Character Recognition) processed versions.

CHAPTER 12: INTERNATIONAL SANCTIONS

12.1 Context and overview of obligations

Targeted financial sanctions (TFS) are designed to restrict the flow of funds and economic resources to specific individuals, entities, and regimes that pose risks to international peace, security, and the integrity of the financial system. Typically imposed by bodies such as the United Nations Security Council and implemented domestically by authorities like the Office of Financial Sanctions Implementation, TFS aim to combat threats including terrorism, proliferation of weapons of mass destruction, and serious human rights abuses. They do this by requiring firms to identify sanctioned parties, freeze their assets, and prevent them from accessing financial services or economic resources, thereby limiting their ability to operate and exert influence.

Targeted financial sanctions compliance starts with strong governance. Senior management must assign responsibility to a reporting officer and maintain a clear, written sanctions policy. Firms should carry out a sanctions specific risk assessment - reviewed at least annually to understand exposure and shape appropriate controls.

Effective screening is central. Firms must screen clients, beneficial owners, and counterparties at onboarding, periodically, and whenever lists update, using sources such as the Office of Financial Sanctions Implementation consolidated list and the Bermuda Sanctions List. Screening tools should be properly configured (including fuzzy matching) and regularly tested. All alerts must be investigated and documented. If a true match is identified, firms must freeze assets, stop activity, avoid tipping-off, and report promptly to the Financial Sanctions Implementation Unit and the supervisory authority, considering a suspicious activity report where relevant.

Firms must also report breaches without delay, provide regular staff training, and keep comprehensive records for at least five years. Ongoing oversight is essential, including annual reporting to senior management, testing of controls, and continuous improvement of the sanction's framework.

The following chapter will provide additional details and guidance on how to implement these international sanctions obligations.

12.2 Legal and Regulatory Framework

- The International Sanctions Act 2003
- The International Sanctions Regulations 2013
- Overseas Territories Orders in Council extending UK and UN sanctions regimes to Bermuda
- The Proceeds of Crime Act 1997 (as amended) (POCA)
- The Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA)

- The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (as amended)

As a British Overseas Territory, Bermuda implements United Nations Security Council sanctions and UK sanctions measures. There are currently dozens of country-based and thematic sanctions regimes in force, listed in the International Sanctions Regulations 2013 and updated periodically through notices published by the UK Office of Financial Sanctions Implementation (OFSI) and Bermuda's FSIU.

12.3 Types of Financial Sanctions

Financial sanctions include:

- **Asset freezes**: Prohibition on dealing with funds or economic resources of designated persons;
- **Financial restrictions**: Limitations on access to financial markets, services or capital;
- **Sectoral sanctions**: Restrictions on specific industries or economic sectors;
- **Trade sanctions**: Prohibitions on import, export or provision of certain goods and services;
- **Directions to cease business**: Requirements to terminate or refrain from business relationships with specified persons, entities or jurisdictions.

12.4 Obligations

Entities owned or controlled by designated persons are treated as if they themselves were designated, even if not explicitly named on a sanctions list. Firms must therefore conduct thorough beneficial ownership analysis as part of sanctions screening.

12.5 Governance, Policies and Procedures

Senior Management Responsibility

Overall responsibility for sanctions compliance must be allocated to a director or senior manager within the firm. Senior management must:

- formally adopt and approve a written sanctions compliance policy;
- ensure that adequate resources, systems and training are provided;
- receive regular compliance reports on the effectiveness of sanctions controls;
- take prompt action to address identified deficiencies; and
- Foster a culture of compliance and ethical conduct.

These measures can be part of broader AML/ATF/CPF compliance measures. Specific mechanisms for sanctions compliance are not necessary.

Reporting Officer

Firms must designate a reporting officer (who may be the same person as the Money Laundering Reporting Officer (MLRO) described in Chapter 6) with responsibility for:

- receiving and assessing internal reports of potential sanctions matches or breaches;
- making external reports to the FSIU and supervisory authorities;
- filing SARs to the FIA where sanctions suspicions also raise money laundering or terrorist financing concerns;
- maintaining records of sanctions screening, alerts, investigations and decisions; and
- liaising with senior management, compliance functions and external authorities.

Sanctions Compliance Policy

The sanctions compliance policy should be documented in writing and integrated with the firm's overall AML/ATF/CPF policies and procedures manual. At a minimum, the policy should address:

- the legal and regulatory framework applicable to the firm;
- the firm's sanctions risk appetite and risk assessment methodology;
- roles and responsibilities of senior management, the reporting officer, compliance and operational staff;
- customer and transaction screening procedures (manual and/or automated);
- procedures for investigating and resolving screening alerts;
- criteria for determining "target matches" versus false positives;
- internal reporting lines and escalation procedures;
- external reporting obligations to FSIU, supervisory authorities and the FIA;
- freezing of assets and cessation of prohibited activities;
- procedures for applying for licenses and exemptions;
- record-keeping and audit trail requirements;
- staff training and awareness programs; and
- periodic review and testing of the effectiveness of controls.

Risk-Based Approach

It should be noted that proliferation financing (PF) controls operate through two complementary mechanisms. First, a risk-based approach requires institutions to identify, assess, and mitigate PF risks by considering factors such as customer profiles, geographic exposure, products, and delivery channels, and to apply controls proportionate to those risks. Second, separate and distinct from this assessment, institutions are subject to

mandatory targeted financial sanctions arising from designations by the United Nations Security Council. Once a person or entity is designated, institutions must implement prescribed measures such as asset freezes and prohibitions on making funds or economic resources available immediately and without applying a risk-based judgment. In this way, the risk-based approach informs how PF risks are managed in general, while sanctions obligations impose specific, non-discretionary actions in relation to listed parties.

As with the overall AML/ATF/CPF framework described in chapter 1, the identification, assessment and mitigation of PF risk should take into account the following factor:

- nature, size and complexity of operations;
- client base (individuals, corporates, trusts, high-net-worth, politically exposed persons);
- services offered (litigation, corporate, trust and estate administration, tax advisory, audit, insolvency);
- geographic exposure (cross-border transactions, clients in high-risk jurisdictions, international corporate structures); and
- delivery channels (face-to-face, remote onboarding, reliance on intermediaries).

Firms should conduct a sanctions-specific risk assessment (or incorporate sanctions risk into their existing enterprise-wide AML/ATF/CPF risk assessment) and document:

- inherent sanctions risks arising from the firm's business model;
- mitigating controls in place (screening, due diligence, monitoring, reporting);
- residual risk after controls are applied;
- risk appetite and tolerance levels; and
- actions to address unacceptable residual risks.

Senior management should review and approve the sanctions risk assessment at least annually, or more frequently if there are material changes in the business, regulatory environment or threat landscape.

12.6 Screening: Customers, Transactions and Timing

Screening Obligations

Sanctions screening is the process of checking names of individuals, entities and other parties against sanctions lists to identify designated persons or entities owned or controlled by designated persons. Screening must be embedded in:

- client and matter acceptance procedures;
- customer due diligence (CDD) processes;

- ongoing monitoring; and
- relevant transaction execution and approval workflows.

What to Screen

At a minimum, firms must screen:

- all prospective clients (individuals and entities) before accepting instructions;
- beneficial owners and persons with control over client entities;
- counterparties to transactions (opposing parties, purchasers, sellers, lenders, borrowers, beneficiaries, transferees, payees);
- key parties to matters (directors, shareholders, settlors, trustees, protectors, executors, administrators, third-party service providers);
- related parties and connected persons where relevant to the transaction or matter; and
- existing clients on an ongoing basis (when sanctions lists are updated, periodically as part of ongoing CDD refresh, or when risk triggers arise).

Firms should also consider screening:

- suppliers, vendors and service providers to the firm itself;
- employees, partners and consultants (pre-employment and ongoing); and
- referrers and introducers of business.

When to Screen

Screening should occur:

At onboarding:

- before accepting new clients or opening new matters;
- as part of initial CDD procedures;
- before executing the first transaction or providing services.

During the relationship:

- whenever sanctions lists are updated (OFSI or FSIU publish new designations or amendments);
- periodically as part of CDD refresh and ongoing monitoring (Chapter 5) frequency should be risk-based but at least annually for higher-risk clients;
- prior to executing significant or high-risk transactions;
- when there are material changes in ownership, control or corporate structure; and

- when red flags or adverse information arise.

At transaction execution:

- before processing payments, transfers of funds or execution of trust distributions;
- before completing corporate transactions (mergers, acquisitions, restructurings, capital raises); and
- before providing advice or services that will enable access to funds or economic resources.

Sources of Sanctions Lists

Firms must screen against:

- the UK Office of Financial Sanctions Implementation (OFSI) Consolidated List, available at:

  https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets;
- The Bermuda Sanctions List maintained by the FSIU, available via: https://www.gov.bm/international-sanctions-measures;
- Where the firm has international operations or clients, other relevant lists such as the UN Consolidated List, US OFAC lists, EU sanctions lists (as appropriate to the firm's risk profile and client base).

Lists are updated frequently - sometimes daily. Firms must ensure they have procedures to:

- monitor for and receive alerts of list updates (via email subscription services, automated feeds, vendor notifications);
- promptly update screening databases or software;
- re-screen existing clients and matters against updated lists; and
- document when lists were last updated and when screening was last performed.

The FSIU offers a free email subscription service to notify of any changes to the UK Sanctions Regime as it applies to Bermuda. You can subscribe at the FSIU website listed above.

12.7 Screening Tools, Technology and Fuzzy Matching

Manual vs. Automated Screening

Firms may use:

- **manual screening**: Reviewing sanctions lists directly and comparing client/party names visually (suitable for very small firms with limited client volumes);
- **automated screening software**: Commercial or in-house systems that match names against sanctions lists using algorithms (suitable for larger volumes, complex structures, or where speed and consistency are required);
- **hybrid approach**: Automated initial screening followed by manual review and investigation of alerts.

The choice of method should be documented and based on:

- the volume and nature of the firm's client base and transactions;
- the complexity of corporate structures and beneficial ownership chains;
- the firm's risk profile and risk appetite; and
- the resources available (budget, staff expertise, IT infrastructure).

Screening Software and System Requirements

Where screening software is used, firms should ensure:

- the system covers all relevant sanctions lists (OFSI, FSIU, and others as appropriate);
- lists are updated automatically and in near-real-time, or the firm has a process to update them promptly;
- the system allows screening of individuals, entities, vessels, aircraft and addresses;
- match results are recorded with date/time stamps and audit trails;
- the system integrates with or is compatible with the firm's client management and CDD systems;
- access is controlled and user activity is logged; and
- business continuity arrangements exist in case of system failure (manual fallback procedures).

Firms should conduct due diligence on software vendors, including:

- vendor reputation, track record and regulatory compliance;
- data sources, update frequency and coverage;
- technical reliability, uptime and support arrangements;

- data security and confidentiality protections; and
- contractual terms, service level agreements and liability provisions.

Fuzzy Matching and Matching Algorithms

Fuzzy matching (also known as approximate string matching) is a technique that identifies potential matches even when names are not identical. It accounts for:

- spelling variations and typographical errors (e.g., "Muhammad" vs. "Mohammed");
- transliteration differences from non-Latin scripts (e.g., Arabic, Cyrillic, Chinese);
- alternative spellings, nicknames and aliases (e.g., "Bill" for "William");
- name order differences (Western vs. Eastern naming conventions);
- punctuation and spacing variations (e.g., "Al-Qaeda" vs. "Al Qaeda" vs. "AL Qaeda");
- diacritics and accents (e.g., "José" vs. "Jose").

Fuzzy matching uses algorithms such as:

- **phonetic matching** (Soundex, Metaphone): Matching based on pronunciation similarity;
- **edit distance** (Levenshtein, Damerau-Levenshtein): Measuring the number of character insertions, deletions or substitutions needed to transform one string into another;
- **token-based matching**: Breaking names into components (tokens) and matching subsets;
- **weighted scoring**: Assigning confidence scores to potential matches based on multiple criteria.

Configuring Match Sensitivity

Screening systems typically allow firms to configure:

- **match threshold**: The minimum similarity score (e.g., 70%, 80%, 90%) required to generate an alert;
- **fuzzy logic settings**: The degree of tolerance for spelling differences and name variations;
- **filtering rules**: Excluding certain categories of matches (e.g., common names, corporate suffixes like "Ltd" or "Inc").

High sensitivity settings (lower thresholds, aggressive fuzzy matching):

- *advantage*: reduces the risk of missing true matches (fewer false negatives);

- *disadvantage*: generates a high volume of false positive alerts, increasing operational burden and review time.

Low sensitivity settings (higher thresholds, strict matching):

- *advantage*: reduces false positives and makes screening more efficient;
- *disadvantage*: increases risk of missing true matches (false negatives) where names are spelled differently or transliterated.

12.8 Calibration and Testing

Firms should:

- calibrate matching settings based on the firm's risk profile, client base and tolerance for false positives vs. false negatives;
- document the rationale for chosen settings (risk-based justification);
- test the system periodically using sample data and known positive and negative cases (quality assurance);
- adjust settings if testing reveals excessive false positives (operational inefficiency) or missed matches (compliance risk);
- ensure senior management and the reporting officer understand the limitations and trade-offs of the chosen configuration.

Example calibration considerations:

Firm Profile	Recommended Approach
High-risk client base (PEPs, complex structures, high-risk jurisdictions)	Higher sensitivity settings to minimize false negatives; dedicate resources to review false positives
Large transaction volumes requiring speed	Moderate sensitivity with well-tuned filters; invest in quality screening software and trained staff
Low-risk, domestic client base with limited international exposure	Standard sensitivity settings; periodic re-calibration and testing
Small firm with limited resources	Consider outsourcing to a reputable provider with proven systems (see section 6.7)

Resolving Alerts: False Positives vs. Target Matches

When a screening alert is generated, the firm must investigate to determine whether it is:

- **false positive**: the person or entity is not the designated person (name similarity is coincidental);
- **target match**: the person or entity is the designated person or is owned/controlled by a designated person.

Investigation should include:

- comparing additional identifying information beyond the name:
  - date of birth or year of birth;
  - place of birth;
  - nationality or citizenship;
  - national identification numbers (passport, national ID, tax ID);
  - addresses (residential, business, registered office);
  - other aliases and known associates;
- reviewing the sanctions list entry for detailed descriptive information;
- checking internal records and CDD files for corroborating or distinguishing details;
- conducting open-source research (internet searches, corporate registries, news media) where appropriate and permissible;
- considering the context and plausibility of the match (e.g., a Bermuda client with a common name matching a designation from an unrelated jurisdiction with no apparent connection).

The investigation and decision must be documented, including:

- the screening alert details (date, time, name matched, list source, match score);
- the information reviewed and sources consulted;
- the rationale for concluding false positive or target match;
- the decision-maker and date of decision;
- actions taken (clearance for false positive; freezing, reporting and escalation for target match).

If uncertain, firms should:

- escalate to senior management or external legal counsel;
- err on the side of caution (treat as a potential target match until definitively cleared);
- contact the FSIU for guidance if needed.

12.9 Reliance and Outsourcing

Consistent with the principles in Chapter 5 (CDD) and Chapter 8 (Outsourcing), firms may:

- rely on group-wide screening systems operated by an affiliated entity;
- outsource screening to a third-party service provider;
- use commercial data vendors for sanctions list data and screening services.

Where reliance or outsourcing is used, the firm must:

- Conduct due diligence on the provider (reputation, expertise, regulatory compliance, systems, controls)
- Enter into a written agreement that clearly defines:
  - the scope of services and performance standards;
  - sanctions lists to be covered and update frequency;
  - match threshold and fuzzy matching settings (aligned with the firm's risk appetite);
  - reporting and alert notification procedures;
  - data security, confidentiality and access controls;
  - audit rights and business continuity arrangements;
  - liability and indemnification provisions;
- retain ultimate responsibility for sanctions compliance (outsourcing does not transfer legal liability);
- maintain access to underlying screening data, match results, audit trails and documentation;
- monitor the provider's performance through periodic reviews, quality testing and compliance reports;
- ensure that the firm's staff understand how the outsourced screening operates and how to escalate and investigate alerts.

Firms should retain the ability to override or supplement outsourced screening where necessary based on the firm's own knowledge and risk assessment.

12.10 Internal Reporting, Matches and Breaches

Internal Reporting Procedures

All staff (fee-earners, support staff, partners, consultants) must be trained to recognize sanctions red flags and to report potential matches or breaches immediately to the reporting officer through the firm's internal reporting channels (consistent with the procedures described in Chapter 6 for suspicious activity reporting).

Red flags that should trigger internal reporting include:

- screening alert indicating a potential name match to a sanctions list;
- client or counterparty operating in or connected to a high-risk or sanctioned jurisdiction;
- unusual secrecy or evasiveness about the source of funds or beneficial ownership;
- use of complex or opaque corporate structures inconsistent with the client's profile;
- transactions involving parties, locations or sectors subject to sanctions;
- client requests to expedite transactions or circumvent normal procedures;
- client or counterparty appears on adverse media or public sources as connected to sanctioned persons or activities;
- requests for legal or accounting services that could facilitate sanctions evasion (e.g., restructuring ownership to obscure sanctioned beneficial owners, using shell companies, routing funds through non-sanctioned intermediaries).

Failure to report suspicions internally may itself constitute an offence. Staff should be encouraged to report in good faith without fear of retaliation, and the firm should protect whistleblowers in accordance with employment law and best practice.

Assessment by the Reporting Officer

Upon receipt of an internal report, the reporting officer must:

- acknowledge receipt and record the report;
- conduct or supervise a thorough investigation (see section 6.6 above on resolving alerts);
- determine whether the alert is:
    - a false positive (name match is coincidental; person/entity is not designated);
    - a target match (person/entity is a designated person or owned/controlled by one);

- a potential sanctions breach (prohibited dealing has occurred or is about to occur);
- a potential money laundering or terrorist financing suspicion requiring a SAR (see section 7.4);

- document the decision and rationale;
- take appropriate action based on the determination (clearance, freezing, external reporting, SAR filing, escalation to senior management).

Target Matches: Immediate Actions Required

If the reporting officer determines that a target match exists, the firm must immediately:

- **freeze funds and economic resources**: the firm must not deal with, make available, or permit access to any funds or economic resources owned, held or controlled by the designated person;
- **cease prohibited activities**: the firm must stop providing services or taking actions that would benefit the designated person or enable them to access funds or economic resources;
- **do not tip-off**: the firm must not inform the client or counterparty that they have been identified as a target match or that assets have been frozen, unless legally required or authorized to do so (consistent with tipping-off prohibitions in Chapter 7);
- **report to the FSIU**: the firm must notify the FSIU as soon as practicable, providing:
  - details of the designated person and the sanctions list entry matched;
  - description of the funds or economic resources held or controlled;
  - the nature of the firm's relationship and the services being provided;
  - any transactions or dealings that have occurred or are proposed;
  - contact information for the reporting officer;
- **report to the supervisory authority**: the firm must also notify the Barristers and Accountants AML/ATF Board;
- **consider whether a SAR is required**: if the circumstances also give rise to suspicion of money laundering or terrorist financing, file a SAR with the FIA (see section 7.4);
- **seek legal advice**: consider obtaining independent legal advice, particularly for complex situations or where there is uncertainty.

12.11 Sanctions Breaches and SARs

Where a sanctions breach has occurred or is suspected, and the circumstances also suggest that:

- the funds or economic resources may represent the proceeds of crime; or
- the client or counterparty may be engaged in money laundering or terrorist financing,

the firm must file a SAR with the FIA in accordance with the procedures described in Chapter 7.

Interaction between sanctions reporting and SARs:

- a target match or sanctions breach does not automatically require a SAR only if there is also suspicion of money laundering or terrorist financing;
- conversely, a SAR relating to suspicious activity may also require sanctions reporting if designated persons are involved;
- firms should assess each case on its facts and, where appropriate, make both types of report;
- the reporting officer should coordinate to ensure consistent information is provided to the FSIU and the FIA, while respecting confidentiality and legal privilege where applicable.

Consent Regime

Where a firm has filed a SAR and wishes to proceed with a transaction or continue providing services (for example, to complete a property sale or execute a trust distribution), the firm must:

- request consent from the FIA through the SAR filing (as described in Chapter 7);
- wait for express consent or for the statutory time to expire before proceeding;
- in the context of sanctions, if the transaction would involve a designated person, the firm will also need to apply for a license from the Minister (see section 8 below).

Firms must not proceed with the transaction without the necessary consent and/or license, even if the client is pressing for completion. Doing so would constitute both a money laundering offence (under POCA) and a sanctions offence.

12.12 Licenses and Exemptions

When a License May Be Required

Where a firm holds or controls funds or economic resources of a designated person, or where the firm needs to make funds or economic resources available to a designated person, the firm may apply to the Minister of Legal Affairs and Constitutional Reform for a license to permit the otherwise prohibited activity.

Common scenarios where a license may be sought:

- payment of reasonable legal fees and disbursements for legal representation;
- payment of reasonable professional fees to lawyers for essential services;
- meeting basic needs of a designated individual (food, rent, medical expenses);
- fulfilling pre-existing contractual obligations entered before designation;

- winding up an estate or trust where a designated person is a beneficiary;
- extraordinary and compelling circumstances (humanitarian grounds, to prevent injustice).

License Application Process

Applications should be submitted to the FSIU, which will process the application and make a recommendation to the Minister. The application should include:

- full details of the applicant (the firm and the reporting officer);
- details of the designated person and the sanctions regime applicable;
- description of the proposed activity and the funds or economic resources involved;
- justification for the license (legal basis, necessity, proportionality);
- supporting documentation (invoices, fee agreements, contractual obligations, evidence of basic needs);
- proposed conditions or safeguards to prevent misuse.

The Minister may grant a license subject to conditions, including:

- limits on the amount or type of funds that may be released;
- restrictions on the use of the funds;
- reporting requirements;
- time limits or expiry dates.

Firms must comply strictly with the conditions of any license granted.

12.13 Training and Awareness

Training Obligations

All relevant staff must receive regular training on sanctions compliance, including:

- the legal and regulatory framework for sanctions in Bermuda;
- the types of sanctions and how they apply to the firm's business;
- how to identify sanctions risks and red flags;
- how to use screening tools and interpret match results;
- how to investigate and resolve alerts (false positives vs. target matches);
- internal reporting procedures and the role of the reporting officer;
- external reporting obligations (FSIU, supervisory authority, SARs to FIA);

- tipping-off prohibitions and confidentiality requirements;
- the consequences of non-compliance (criminal, regulatory, reputational);
- case studies and practical scenarios relevant to the firm's practice areas.

Training Frequency and Records

Training should be provided:

- at induction for all new staff;
- at least annually for all existing staff;
- more frequently for higher-risk roles (client-facing staff, CDD and onboarding teams, compliance officers);
- on an ad hoc basis when there are significant changes to sanctions laws, lists or the firm's procedures.

The firm must maintain records of:

- training materials and content;
- dates of training sessions;
- attendance records and participant names;
- assessment or testing results (if used);
- refresher and update training.

Training records should be retained in accordance with Chapter 8 (at least five years from the end of the business relationship or transaction).

Senior Management and Specialist Training

Senior management, the reporting officer, and compliance staff should receive enhanced or specialist training covering:

- advanced sanctions risk assessment techniques;
- complex ownership and control analysis;
- screening technology and calibration;
- investigation and decision-making in ambiguous cases;
- liaison with competent authorities and license applications;
- legal and regulatory developments;
- lessons learned from enforcement actions and case law.

Firms may deliver training in-house or engage external trainers, legal counsel or industry associations to provide specialist sessions.

12.14 Documentation and Record-Keeping

Records to Be Maintained

In accordance with Chapter 8, firms must maintain comprehensive records of sanctions compliance activities, including:

- **policies and procedures**: current and superseded versions of the sanctions compliance policy, with dates of adoption and review;
- **risk assessments**: sanctions-specific risk assessments or sections of the enterprise-wide risk assessment;
- **screening records**:
  - dates and times of screening (at onboarding, periodic refresh, list updates);
  - names and details of persons/entities screened;
  - screening results (matches and non-matches);
  - match alerts and scores;
- **alert investigations**: documentation of the investigation and resolution of each alert, including:
  - the alert details and match information;
  - additional information reviewed (dates of birth, addresses, identifiers, open-source research);
  - analysis and decision (false positive or target match);
  - name of decision-maker and date;
  - actions taken;
- **internal reports**: records of all internal sanctions reports made by staff to the reporting officer;
- **external reports**: copies of reports to the FSIU, supervisory authority, and SARs to the FIA (where applicable);
- **freezing actions**: details of funds or economic resources frozen, dates, amounts, and ongoing status;
- **license applications and grants**: correspondence, applications, supporting documents, licenses received, and compliance with license conditions;
- **training records**: as described in section 9.2;
- **systems and vendor due diligence**: documentation of screening software, vendor agreements, due diligence on providers, system testing and calibration;
- **compliance reports**: periodic reports to senior management on the effectiveness of sanctions controls, statistics, incidents, and remedial actions;

Retention Periods

Sanctions compliance records must be retained for:

- at least **five years** from the end of the business relationship or the completion of the transaction;
- longer where required by other laws or regulations (e.g., legal professional privilege, litigation hold, regulatory investigation);
- in accordance with the firm's general record retention policy and Chapter 8 requirements.

Records should be maintained in a format that allows retrieval and production to competent authorities upon request, and must be protected against loss, damage, alteration or unauthorized access.

12.15 Reviewing Effectiveness

Periodic Review and Testing

Senior management must ensure that the effectiveness of sanctions compliance controls is reviewed and tested periodically. This should include:

- **annual compliance reports** from the reporting officer or compliance function, covering:
  - number and nature of screening alerts generated;
  - number of false positives vs. target matches;
  - number and outcome of investigations;
  - external reports made to FSIU, supervisory authority and FIA;
  - license applications submitted and outcomes;
  - training completion rates and effectiveness;
  - system performance and vendor reliability;
  - incidents, breaches and remedial actions;
  - recommendations for improvements;
- **sample testing** of screening alerts and investigations to assess quality and consistency of decision-making;
- **system testing** to ensure screening software is functioning correctly, lists are up to date, and match settings are appropriate;
- **benchmarking** against peer firms, industry guidance and regulatory expectations;
- **independent review** by internal audit, external auditors, or specialist consultants (risk-based and proportionate to firm size and complexity).

12.16 Continuous Improvement

Firms should:

- identify and implement improvements to policies, procedures, systems and training based on review findings;
- monitor changes in sanctions laws, regulations, lists and guidance;
- stay informed of enforcement actions, case law and industry developments;
- engage with industry associations, professional bodies and peer firms to share best practice;
- foster a culture of continuous improvement and learning.

Senior management should ensure that adequate resources are allocated to address identified deficiencies and that remedial actions are tracked and completed.

12.17 Summary of Key Obligations

Obligation	Key Actions
Governance	Allocate responsibility to senior management and a reporting officer; adopt written sanctions policy
Risk assessment	Conduct sanctions-specific risk assessment, review annually
Screening	Screen clients, beneficial owners and counterparties at onboarding, periodically and when lists update
Lists	Use OFSI consolidated list and Bermuda Sanctions List; monitor for updates
Technology	Use appropriate screening tools; configure fuzzy matching; test and calibrate
Alerts	Investigate alerts thoroughly; document decision (false positive or target match)
Target match	Freeze funds; cease activity; do not tip off; report to FSIU and supervisory authority; consider SAR
Breach	Report to FSIU and supervisory authority; file SAR if money laundering/TF suspected; seek consent/license
Training	Provide initial and annual training to all staff; enhanced training for key roles
Records	Maintain comprehensive records; retain for at least five years
Review	Annual compliance reports to senior management; test effectiveness; continuous improvement

Further Information and Contact Details

Financial Sanctions Implementation Unit (FSIU)

Email: fsiu@gov.bm

Tel: +1 441-292-4595

Website: https://www.gov.bm/international-sanctions-measures

Barristers and Accountants AML/ATF Board

Website: https://www.amlatfboard.bm

Financial Intelligence Agency (FIA)

Suspicious Activity Report filings: https://www.fia.bm

Tel: +1 441-278-0300

UK Office of Financial Sanctions Implementation (OFSI)

Consolidated List: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

Email: OFSI@hmtreasury.gov.uk

ANNEX 1 - RISK MITIGATION MEASURES

Risk mitigation measures for high-risk situations may include:

- increased awareness of higher risk situations within business lines across the entity;
- increased monitoring of transactions;
- the approval of the establishment of relationships is escalated to senior management;
- the levels of on-going controls and reviews of relationships are increased;
- personnel that have clear lines of authority, responsibility and accountability;
- adequate segregation of duties (for example, an employee establishing a relationship with a client is not authorized to also approve it as that authorization is the responsibility of someone else in the organization);
- proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold must follow a procedure to get approval for the transaction by someone else in the organization);
- internal reviews to validate the risk assessment processes;
- seeking additional information beyond the minimum requirements to substantiate the client's identity or the beneficial ownership of an entity;
- obtaining additional information about the intended nature of the relationship, including estimates regarding the amount and type of business activity;
- obtaining additional documented information regarding the client' source of funds and accumulation of wealth;
- requesting high risk clients to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
- getting independent verification of information (i.e. from a credible source other than the client);
- stopping any transaction with a potential client until identification information has been obtained;
- implementing an appropriate process to approve all relationships identified as high risk as part of the client acceptance process or declining to do business with potential clients because they exceed your risk tolerance level;
- implementing a process to exit from an existing high-risk relationship which is beyond the entity's stated risk tolerance level; and
- analyzing money laundering, terrorist and proliferation financing risk vulnerabilities for new acquisition processes.

ANNEX 2 - MONEY LAUNDERING, TERRORIST AND PROLIFERATION FINANCING RED FLAGS FOR THE ACCOUNTANCY SECTOR

1. The Regulations require firms to conduct ongoing monitoring of business relationships and take steps to be aware of transactions with heightened money laundering, terrorist and proliferation financing risks. Firms are required to report suspicious transactions and activity.

2. This section highlights several warning signs for accountants generally and for those working in specific business areas to help firms decide where there are reasons for concern or the basis for a reportable suspicion.

3. Because money launderers, terrorist and proliferation financiers are always developing new techniques, no list of examples can be fully comprehensive. However, the following are some key factors indicating activity or transactions which might heighten a client's risk profile or give cause for concern.

Non-Transparent clients

4. Whilst face to face contact with clients is not always possible, an excessively obstructive or secretive client may be a cause for concern. Consideration should be given as to whether clients who demand strict confidentiality relating to their financial and business affairs are evading tax or seeking to mask the true beneficial ownership of their assets.

Unusual instructions

5. Instructions that are unusual in themselves, or for the firm or the client may give rise to concern, particularly where no rational or logical explanation can be given. Be wary of:
    i. loss-making transactions where the loss is avoidable;
    ii. dealing with money or property when there are suspicions that it is being transferred to avoid the attention of either a trust in a bankruptcy case, a revenue authority, or a law enforcement agency;
    iii. complex or unusually large transactions, particularly where underlying beneficial ownership is difficult to ascertain and/or where the underlying transactions have been conducted in cash;
    iv. unusual patterns of transactions which have no apparent economic purpose particularly those where several jurisdictions and different entities are involved for no logical business reason;
    v. funds that are being switched between investments or jurisdictions for no apparent reason;
    vi. use of shell companies, blind trusts or other structures that are merely being used as a front for other activities; and
    vii. excessive use of off-balance sheet transactions or activity.

Instructions outside the firm's area of expertise

6. Taking on work which is outside the firm's normal range of expertise can present additional risks because money launderer might be using the firm to avoid answering too many questions. An inexperienced accountant might be influenced into taking steps which a more experienced accountant would not contemplate. Accountants should be wary of highly paid niche areas of work in which the firm has no background, but in which the client claims to be an expert. If the client is based outside Bermuda, firms should satisfy themselves that there is a genuine legitimate reason why they have been instructed. For example, have the firm's services been recommended by another client or is the matter based near your firm? Making these types of enquiries makes good business sense and a sensible AML/ATF/CPF check.

Changing instructions

7. Instructions that change unexpectedly might be suspicious, especially if there seems to be no logical reason for the changes. The following situations could give rise to cause for concern:
    i. client deposits funds into a firm's client account, but then ends the transaction for no apparent reason;
    ii. a client advises that funds are coming from one source and at the last minute the source changes; or
    iii. a client unexpectedly requests that money received into a firm's client account be sent back to its source, to the client or to a third party.

Use of client accounts

8. Client accounts should only be used to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting criminal money through a professional firm's client account can clean it, whether the money is sent back to the client, on to a third party, or invested in some way. Introducing cash into the banking system can become part of the placement stage of money laundering. Therefore, the use of cash for noncash-based businesses is often a warning sign.

Source of funds

9. If funding is from a source other than a client, firms may need to make further enquiries, especially if the client has not advised what they intend to do with the funds before depositing them into the firm's account. If it is decided to accept funds from a third party, perhaps because time is short, firms should ask how and why the third party is helping with the funding. Enquiries do not need to be made into every source of funding from other parties. However, firms must always be alerted to warning signs and in some cases will need to seek more information.

Holding funds

10. Firms who choose to hold funds as stakeholder or escrow agent in commercial transactions should consider the checks to be made about the funds they intend to hold before the funds are

received. Consideration should be given to conducting CDD measures on all those on whose behalf the funds are being held. Consideration should be given to any proposal that funds are collected from several individuals whether for investment purposes or otherwise. This could lead to wide circulation of client account details and payments being received from unknown sources.

Accountancy and audit services

11. Except for certain strict liability offences, criminal conduct requires an element of criminal intent which means that an offender must know or suspect that an action or property is criminal. Conduct which is an innocent error or mistake may be criminal where it constitutes a strict liability offence but does not mean it will also be money laundering. If an individual or firm knows or believes that a client is acting in error, the client may be approached and the situation and legal risks explained to them. However, once the criminality of the conduct is explained to the client, they must bring their conduct (including past conduct) promptly within the legislation to avoid a money laundering offence being committed. Where there is uncertainty about the legal issues that are outside the competence of the firm, clients should be referred to an appropriate specialist or legal adviser. If there are reasonable grounds to suspect that a client knew or suspected that their actions were criminal, a report must be made. Even if the client does not have the relevant intent, but the firm is aware that there is criminal property, consideration needs to be given to whether a report must be made to the FIA.

General warning signs

12. Any of the following general warning signs should prompt additional questions or investigation by those offering accountancy and audit services:
    i. use of many different firms of auditors and advisers for connected companies and businesses;
    ii. the client has a history of changing bookkeepers or accountants yearly; and
    iii. company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues to operate without reasonable explanation of the continued loss.

Factors arising from action by the entity or its directors

13. Where an entity is actively involved in money laundering, terrorist and proliferation financing, the signs are likely to be similar to those where there is a risk of fraud, and include:
    i. unusually complex corporate structure where complexity does not seem to be warranted;
    ii. complex or unusual transactions, possibly with related parties;
    iii. transactions with little commercial logic taking place in the normal course of business (such as selling and re-purchasing the same asset);

iv. transactions conducted outside of the normal course of business or where the method or payment/receipt is not usual business practice, such as wire transfers or payments in foreign currency;

v. transactions where there is a lack of information or explanation, or where explanations are unsatisfactory;

vi. transactions that are undervalued or overvalued, including double billing;

vii. transactions with companies whose identity or beneficial ownership is difficult to establish;

viii. abnormally extensive or unusual related party transactions;

ix. unusual numbers of cash transactions for substantial amounts or many small transactions that add up to a substantial amount;

x. payment for unspecified services or for general consultancy services; and

xi. long delays in the production of company or trust accounts for no apparent reason.

The client may be unknowingly a party to money laundering

14. There may be occasions where the client has been duped by its own clients or clients into providing assistance or a vehicle for laundering criminal funds. Warning signs may be:

i. unusual transactions without an explanation or a pattern of trading with one client that is different from the norm;

ii. request for settlement of sales in cash;

iii. a client setting up a transaction that appears to be of no commercial advantage or logic;

iv. a client requesting special arrangements for vague purposes;

v. unusual transactions with companies registered overseas;

vi. request for settlement to bank accounts or jurisdictions which would be unusual for a normal commercial transaction; or

vii. excessive overpayment of accounts, subsequently requesting a refund.

Administration of estates

15. A deceased person's estate is very unlikely to be actively utilized by criminals as a means for laundering their funds; however, there is still a low risk of money laundering for those working in this area where estate assets have been earned or are located in a higher risk territory, firms may need to make further checks about the source of those funds.

16. When winding up an estate, there is no blanket requirement that firms should be satisfied about the history of all the funds which make up the estate under administration. However, firms should be aware of the factors which can increase money laundering risks and consider the following:

i. where estate assets have been earned in a foreign jurisdiction, firms should be aware of the wide definition of criminal conduct in POCA; and

ii. where estate assets have been earned or are in a higher risk territory, firms may need to make further checks about the source of those funds.

17. Firms should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion or reasonable grounds for suspicion is formed and problems of delayed consent can be avoided.

18. Firms should bear in mind that an estate may include criminal property. An extreme example would be where the firm knows or suspects or has reasonable grounds to suspect that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime. If firms know or suspect or have reasonable grounds to suspect that the deceased person improperly claimed benefits/allowances or had evaded the due payment of taxes during their lifetime, criminal property will be included in the estate and so a money laundering disclosure may be required.

19. Relevant local laws will apply before assets can be released. Firms should remain alert to warning signs, for example if the deceased or their business interests are based in a higher risk jurisdiction.

20. If the deceased person is from another jurisdiction and an accountant is dealing with the matter in the home country; firms may find it helpful to ask that person for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate.

Charities

21. While most charities are used for legitimate reasons, they can be used as money laundering, terrorist and proliferation financing vehicles. Firms acting for charities should consider its purpose and the organization's it is aligned with. If money is being received on the charity's behalf from an individual or a company donor, or a bequest from an estate, firms should be alert to unusual circumstances, including large sums of money.

Business recovery or receiverships

22. Insolvency practitioners will often encounter criminal activity when winding up or effecting recovery for a business. Serious fraud which has resulted in benefit either for the business or an individual will be reportable to the FIA as will incidences where the business has been used to launder the proceeds of crime. Examples may be where:

i. fraud has caused or contributed to the failure of the business;

ii. there has been illegal siphoning off or transfer of assets by directors/shareholders;

iii. false accounting or misrepresentation of profits has been applied to maintain share value;

iv. the Directors or members of senior management have been guilty of illegal trading or market abuse and;

v. tax fraud has been committed by reducing income or profits.

Observation of unlawful conduct resulting in advice

23. It should be borne in mind that for property to be criminal property (property which is or in whole or in part directly or indirectly represents proceeds of criminal conduct), not only must it constitute a person's benefit from criminal conduct, but the alleged offender must know or suspect that the property constitutes such a benefit. This means, for example, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not criminal property, and no money laundering offence has arisen until the offender becomes aware of the error. Examples of unlawful behavior which may be observed, and may well result in advice to a client to correct an issue, but which are not reportable as money laundering, are set out below:

    i. offences where no proceeds or benefit results, such as the late filing of company accounts. However, firms should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position;

    ii. misstatements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due;

    iii. attempted fraud where the attempt has failed and so no benefit has accrued (although this may still be an offence in some jurisdictions e.g. the UK); and

    iv. where a client refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, firms should consider what that indicates about the client's intent and whether the property has now become criminal property.

Proliferation Financing Warning Signs

24. In addition to the ML/TF warning signs described above, firms should be alert to the following indicators of potential proliferation financing:

    i. transactions involving goods, technology, or materials that could have dual-use applications (civilian and military), particularly where the stated end-use does not appear consistent with the nature of the goods;

    ii. unusual shipping or logistics arrangements, including complex or illogical shipping routes, frequent changes to shipping documentation, or the use of free trade zones to obscure the origin or destination of goods;

    iii. clients or transactions with links to designated persons or entities under UNSCR 1718 (DPRK) or UNSCR 2231 (Iran), or to persons or entities acting on their behalf or at their direction;

iv. use of front companies, shell companies, or complex corporate structures to obscure connections to sanctioned jurisdictions or designated persons, including the use of nominees to disguise beneficial ownership;

v. reluctance by clients to provide end-user certificates or information about the ultimate destination of goods or services, or the provision of incomplete or inconsistent information;

vi. transactions with no apparent economic rationale involving jurisdictions with known proliferation risks, particularly the DPRK, Iran;

vii. requests to establish complex trust or corporate structures in jurisdictions with strong secrecy provisions, where the underlying commercial rationale is unclear or appears inconsistent with the client's profile; and

viii. any other indicators identified in the FSIU Bermuda CPF Guidance (May 2025), including trade-based indicators such as falsified documentation, inconsistent descriptions of goods, and payments routed through multiple jurisdictions to obscure the ultimate beneficiary.