GUIDANCE FOR THE ACCOUNTANCY PROFESSION ON ANTI-MONEY LAUNDERING AND COUNTERING TERRORIST FINANCING

October 2019

Contents

A. INTRODUCTION AND OBJECTIVE

1. Accountants are key gatekeepers for the financial system, facilitating vital transactions and information that underpin the Cayman Islands economy. As such, they have a significant role to play in ensuring their services are not used to further a criminal purpose. The fight against crime demands that criminals be prevented from legitimising the proceeds of their crime by the process of "money laundering". It is a process which can involve many institutions outside the more obvious targets of banks, other credit institutions and bureaux de change. Professionals such as accountants and lawyers are at risk because their services could be of value to the successful money launderer who often seeks to involve many other, often unwitting 'accomplices'.
2. This guidance is based on the Law and AML Regulations as of 1 October 2019.
3. Accounting Firms are required to register with CIIPA and information can be found in CIIPA's *Helpsheet: Registration of Accountancy Services Firms*
4. This Guidance is designed to cover relevant financial business activity of Accounting Firms. The full list of activities is prescribed in Schedule 6 of the Proceeds of Crime Law.
5. However, those registered accountancy firms that are not conducting relevant financial business may opt to observe the guidance for risk management purposes.
6. Further, whilst, the Cayman Islands anti-money laundering and countering terrorist financing ("AML/CFT") regime applies only to relevant financial business services, some Firms will find it easier to apply certain AML/CFT controls to all of the services that they offer, but this is a decision for the firm as it can be unnecessarily costly to apply AML/CFT controls to services that do not fall within the AML/CFT regime.
7. No penalties or enforcement will apply to firms that are not conducting relevant financial business other than where an accounting firm fails to register with CIIPA.

Legislation

8. The legislation which comprises the Cayman Islands AML/CFT regime is contained in:

The Proceeds of Crime Law (2019 Revision) ("POCL")	Contain the offences that can be committed by individuals or organisations.
The Terrorism Law 2018 ("TL")	
The Anti Money Laundering AML Regulations 2018 ("the AML Regulations")	Prescribe the controls that Firms conducting "relevant financial business" are obliged to implement, as well as the

	related offences that can be committed by Firms and key individuals within them. Designates CIIPA as AML Supervisor and prescribes its powers and

CIIPA's Role as Supervisor

9. On December 13, 2017 CIIPA became the AML Supervisory Authority for accounting firms and is charged with:
    a. registering all accounting firms,
    b. monitoring and acting to ensure compliance with the Law and Regulations for those firms carrying on relevant financial business, and
    c. issuing guidance, directives and procedures.

10. The empowering legislation was the Anti Money Laundering (Designated Non-Financial Businesses and Professions) (Amendment) (No2) Regulations, 2017 ("DNFBP Regs") which amended the then Anti-Money Laundering Regulations 2017 ("AMLRs") now the Anti-Money Laundering Regulations (2018 Revision).

Status of this guidance

11. CIIPA issues this guidance in order to **promote compliance with the AML Regulations** (see Regulation 55D (1)(c)).
12. Where this guidance identifies high Money Laundering ("ML") or Terrorist Financing ("TF") risk, firms are required to apply enhanced due diligence in those cases (Regulation 27(b)).
13. CIIPA may take into account whether a firm has complied with this Guidance:
    a. To determine whether to take **enforcement action** under the AML Regulations (Regulation 56(4)(b)) and
    b. As a relevant factor in the **level of fines** to be imposed in the event of breach of the AML Regulations (Regulation 55V(1)).
14. A **court** determining an allegation of a breach of the Regulations may take account of whether the Firm complied with this Guidance (Regulation 56(2)).
15. If a professional body is called upon to judge whether a member has complied with its general **ethical or professional conduct** requirements, it may be influenced by whether or not the member has applied the provisions of this guidance.

Other AML Supervisors ("Dual supervised")

16. Per the AML Regulations, there may be cases where a Firm could be supervised by more than one AML Supervisor. For example, a firm may offer accounting services and also act as a company manager licensed and supervised by the Cayman Islands Monetary Authority. In those cases, the AML Supervisors will agree to coordinate supervision or that one Supervisor will be the lead.

Dual Supervision: The AML Supervisors will cooperate directly and eventually by means of a Multilateral Memorandum of Understanding to avoid duplicating supervision.

17. In either case, Firms may use AML guidance issued by other supervisors where that guidance is better aligned with the specific circumstances faced by the Firm. Where the Firm follows guidance other than herein, it must be in a position to **justify** this approach.
18. The AML Supervisors are:
    a. Cayman Islands Institute of Professional Accountants ("CIIPA")
    b. Cayman Islands Monetary Authority ("CIMA")
    c. Department of Commerce and Industry ("DCI")
    d. Cayman Islands Legal Practitioners Association ("CILPA")
    e. General Registry: Supervisor of Non-Profit Organisations
19. Note that the Financial Reporting Authority ("FRA") is an important institution. It is not an AML Supervisor, it is the Financial Intelligence Unit to which suspicious activity reports are filed and also charged with ensuring the implementation of targeted financial sanctions with respect to terrorism, terrorism financing, proliferation, proliferation financing, and other restrictive measures related to anti-money laundering (AML) and combatting the financing of terrorism (CFT) and proliferation (CFP) from and within the Cayman Islands. See http://www.fra.gov.ky/contents/page/1 and Section E for more information on reporting to the FRA.

Penalties and Enforcement

20. The AMLRs provide for administrative fines to be imposed on firms in breach (Regulation 55R(2)) which shall be determined based on whether classed as minor, serious or very serious as prescribed in Schedule 2 of the Regulations and in summary are:

Minor	*Serious*	*Very Serious*
Failure to provide information (Reg 53A)	Failure to implement controls (Reg 5 except (b))	Failure to implement controls for identification and recordkeeping

		(Reg 5(b))
Failure to Allow Onsite Visit (Reg 55M)	Failure to register (Reg 55F)	
Providing false information (Reg 55O)		

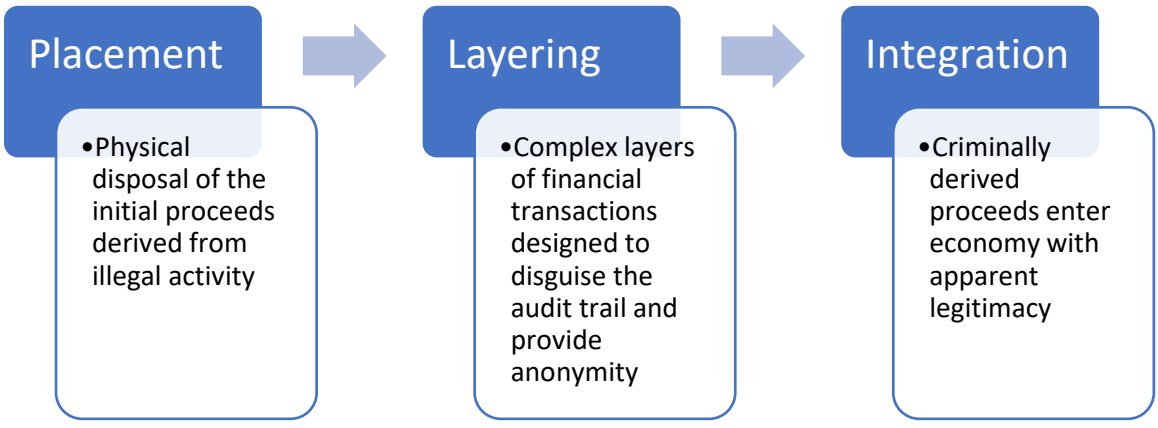
21. For a minor breach the fine is $5,000 and $5,000 for each continuing breach up to a maximum of $20,000.
22. For a serious breach the fine maximum amount is $50,000 for an individual and $100,000 for a firm.
23. For a very serious breach the fine maximum amount is $100,000 for an individual and $1,000,000 for a firm.
24. CIIPA has discretion as to the actual amount of the fine for serious and very serious breaches up to the maximums but that discretion must be exercised taking account of relevant factors and:
    a. Three Principles- Disgorgement, Punitive and Deterrence (see Regulation 55V)
    b. Criteria set out in Regulations 55X and 55Y, including consideration of the nature and seriousness of the breach and your firm inadvertence, intent or negligence in committing the breach.
25. CIIPA may alternatively refer the matter to the Director of Public Prosecutions.
26. CIIPA may also initiate simultaneously or subsequently investigation and disciplinary proceedings against an individual that is a CIIPA member or Firm (see Section 18 of the Accountants Law).
27. For more information on the enforcement processes see *Helpsheet – Supervision and Enforcement.*

What is money laundering?

28. Money laundering is defined widely. It includes all forms of using or possessing criminal property (as well as facilitating the use or possession) regardless of how it was obtained.
29. Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows

them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of funds. Their "dirty" funds come to appear "clean".

30. Money laundering is a global phenomenon that affects all countries in varying degrees. By its very nature it is a hidden activity and therefore the scale of the problem and the amount of criminal money being generated either locally or globally each year is impossible to measure accurately. However, failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime a more attractive proposition.
31. There is no one method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a car or jewellery) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). Initially, however, in the case of drug trafficking and some other serious crimes such as human trafficking and bribery, the proceeds usually take the form of cash which needs to enter the financial system by some means. Street level purchases of drugs are almost always made with cash.
32. Despite the variety of methods employed, the laundering process is typically accomplished in three stages which may comprise numerous transactions by the launderers that could raise suspicions of underlying criminal activity:



33. The three basic steps may occur as separate and distinct phases, they may occur simultaneously or, overlap.

Risks to Accountants

34. Money launderers are plausible people and their business activities will often be difficult to distinguish from those of the legitimate client. Like the legitimate client, the launderer may need audit services and a whole range of financial, tax and business advice and support. Some areas of an accountant's work may be more vulnerable than others to the involvement of money launderers, but no area is immune.
35. Criminal proceeds can take many forms. Cost savings (as a result of tax evasion or ignoring legal requirements) and other less obvious benefits can be proceeds of crime. Where criminal property is used to acquire more assets, these too become criminal property.
36. If someone knowingly engages in criminal activity, but does not succeed in benefitting from it, then he may have committed some offence other than money laundering (it will often be fraud) and whilst there may be no obligation to make a money laundering report, Firms and individuals should nonetheless consider whether they are under some other professional reporting obligations.
37. Criminal property may take any form, including:
    a. money or money's worth,
    b. securities,
    c. a reduction in a liability, and
    d. tangible or intangible property.
38. Money laundering can involve the proceeds of offending in the Cayman Islands but also of conduct overseas that would have been an offence had it taken place in the Cayman Islands.
39. For the purposes of this guidance money laundering also includes terrorist financing.

Offences

40. The primary money laundering offences defined under POCL can be committed by anyone, whether conducting relevant financial business or not but the AML Regulations impose specific provisions on those conducting relevant financial business.
41. Money laundering offences are defined by POCL, as activity designed to:
    a. **conceal**, disguise, convert or transfer or remove criminal property (section 133);
    b. enter into, or become involved in, an **arrangement** which they know or suspect facilitates money laundering; (section 134); or
    c. **acquire**, use or possess criminal property (section 135).

42. A firm could commit the s134 offence if it agreed to act, or continued to act, for a client which it knew or suspected to be engaged in laundering the proceeds of any criminal conduct. This is because the firm would be enabling the client to present an appearance of legitimacy, so allowing money laundering to continue.
43. Any of these offences is punishable by up to 14 years' imprisonment and/or an unlimited fine.

Defences: Primary Offences

44. None of these offences is committed if:

    a. the persons involved did not know or suspect that they were dealing with the proceeds of crime; or

    b. a report of the suspicious activity is made to the FRA under the provisions of POCL (as a suspicious activity report, or SAR); or

    c. there is a reasonable excuse for not reporting (this is likely to be defined narrowly, so very rare); or

    d. the conduct which gave rise to the criminal property happened in a location where it was legal (i.e., outside the Cayman Islands) but the requirements of this exception are complex, onerous and stringent; specialist legal advice may be needed.[1]

45. The following offences apply and are of greater concern to the unwitting or coerced accountant:

    a. Failure to report a suspicion of money laundering or terrorist financing.

    b. Disclosing that a suspicious activity report has been made, or is being contemplated, in a way that is likely to prejudice any subsequent investigation ('tipping off').

46. A tipping off offence cannot arise unless the person concerned knows or should suspect that an activity that should be reported is taking place, has taken place or about to take place and he makes a disclosure likely to prejudice an investigation. Therefore, preliminary enquiries of a prospective client where a firm seeks additional information will not trigger a tipping off offence unless or until the enquirer has knowledge or reasonable grounds for suspicion of a current or impending investigation either internally or by the FRA. However, if the enquiries lead to a subsequent report being made, then the client must not be informed or alerted.

[1] The equivalent offences under the Terrorism Law 2018 (TL) do not have this exemption.

Defences: Failure to Report

47. In the case of a person who is employed by a Firm to which the Regulations apply, internal reporting in accordance with the procedures laid down by the firm will be a defence to a charge of failing to report. Reports should be made internally (see Section E.)
48. However, Partners should note that this defence of having made an internal report, may not be available to them if they are not "in employment". In that case, a partner should ask the MLRO to confirm that a report has been made to Reporting Authority, unless the MLRO can convince the partner that the suspicion is groundless. If unconvinced by the MLRO, the partner has a personal legal obligation to make the report him/herself.

What is Terrorist Financing?

49. Terrorism is an unlawful action which is intended to compel a government or an international organisation to do or refrain from doing any act; or intimidate the public or a section of the public, for the purpose of advancing a political, religious, racial or ideological cause; or a terrorist financing offence.
50. These actions include any which causes or is likely to cause -
    a. loss of human life or serious bodily harm;
    b. damage to property; or
    c. prejudice to national security or disruption of public safety including disruption in the provision of emergency services or to any computer or electronic system or to the provision of services directly related to banking, communications, infrastructure, financial services, public utilities, transportation or other essential infrastructure.
51. By contrast, financial gain is the main objective of other types of financial crimes. Nonetheless, terrorist groups, like criminal organisations, must develop sources of funding, a means of laundering those funds, and a way of using those funds to obtain materials and logistical items to commit terrorist acts.

Terrorism is not necessarily expensive business. The London public transport bombings that took place in July 2005 are estimated to have cost a mere £8k. The price tag on the January 2015 shootings at Charlie Hebdo in Paris is thought to be less than $20k. The fact that we are not looking at large amounts of money changing hands makes terrorist financing that much more difficult for an accountant to spot, but not impossible, especially as we may well see numerous financial transactions during a single engagement.

52. Sources of funding for terrorism could be unlawful sources such as kidnapping, extortion, smuggling, various types of fraud (, theft, robbery, narcotics trafficking, DVD pirating, counterfeiting, cigarette smuggling, credit card fraud, and small scale drugs trade. Firms must be aware however, that funding for terrorist groups, unlike for criminal organisations, may also include funds derived from legitimate sources or from a combination of lawful and unlawful sources. This funding from legal and legitimate sources is a key difference between terrorist groups and traditional criminal organisations.

> "… the methods of moving money may well be quick and simple [rather than] complicated transaction structures. Methods include cash mules, pre-paid gift cards, pre-paid credit cards and diversion of charitable funds. Slightly more elaborate is the possible use of online gambling or MMORPGs (Massive Multiplayer Online Role Playing Games) that use virtual money (or credits) that players can exchange for real currency. Such games include, for example, World of Warcraft. Not only are transactions between avatars, but the small amounts are relatively inconspicuous. Yet they allow users to pay virtual money to their associates anywhere in the world, who can then take steps outside the system to convert it into local currency."
>

53. Terrorist groups find ways of laundering the funds in order to disguise links between them and their funding sources, and to be able to use the funds without drawing the attention of authorities.

54. Charities or other non-profit organizations ("NPOs") are also vulnerable and could be misused for Terrorist Financing ("TF"). Terrorist groups use NPOs to raise and launder funds for terrorism.

> "….. facilitating [terrorist financing] …may be unwitting or complicit. e.g. BNP Paribas processing transactions involving sanctioned entities in Sudan despite being in violation of U.S. law. Internal emails referred to historical relationships with significant commercial stakes and that the compliance team did not want to stand in the way of maintaining such business. Contrast that scenario with that of a money service business, transferring funds between two individuals with no known connection to terrorist organisations. A vast spectrum lies in between, and as accountants we are also subject to commercial pressures, but we also have codes of ethics that are there to protect us"
>

55. The Terrorism Law applies to actions, persons, or property, both inside and outside of the Cayman Islands. Any person who believes or suspects that another person has committed an offence under this law must disclose the information to the Financial Reporting Authority ("FRA") or to the police as soon as is reasonably practical. Failure to do so is an offence and is punishable- (a) on summary conviction, to imprisonment for two years and a fine of four thousand dollars; or (b) on conviction on indictment, by imprisonment for five years, and to a fine. The Court may also make a forfeiture order.

What are Financial Sanctions?

56. Firms have obligations under different international targeted financial sanctions/orders, and designations and directions issued in relation to TF and Proliferation Financing ("PF") as applicable. United Nations and European Union sanctions are implemented in the Cayman Islands by way of Overseas Orders in Council.
57. Firms must take action such as filing suspicious activity reports, freezing funds, and informing the Financial Reporting Authority as required under the relevant Orders if they discover a relationship that contravenes any applicable sanctions orders or directions.

What is Proliferation Financing?

58. PF refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans- shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, radiological or biological weapons and their means of delivery and related materials (including both technologies and dual use of goods used for illegitimate purposes), in contravention of national laws or, where applicable, international obligations. See the Proliferation Financing (Prohibition) Law, 2017, ("PFPL").
59. The TL also deals with matters relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. The TL makes it an offence to provide, receive or invite instruction or training in the making or use of-(a) firearms; (b) explosives; or (c) chemical, biological or nuclear weapons.
60. For applicable international targeted financial sanctions in relation to terrorism and, proliferation, Firms should refer to the website of the FRA especially the FRA's Industry Guidance - *Targeted Financial Sanctions with Respect to Terrorism, Terrorist Financing, Proliferation, and Proliferation Financing within the Cayman Islands*.

B. RESPONSIBILITY AND GOVERNANCE

61. Good governance in Firms is essential for effective internal controls.
62. For Firms conducting *relevant financial business,* the AML *Regulations* require systems and controls to mitigate and manage ML and TF risk. The Regulations impose a duty to ensure that relevant staff are kept aware of these controls and are trained to apply them properly.
63. If a Firm fails to meet its obligations under the AML Regulations, civil penalties and/or criminal sanctions can be imposed on the Firm and any individuals deemed responsible.[2] This could include anyone in a senior position who neglected their own responsibilities or agreed to something that resulted in the compliance failure.

Anti-Money Laundering Compliance Officer and Money Laundering Reporting Officer

64. Regulation 3 requires the appointment of an Anti-Money Laundering Compliance Officer ("AMLCO') and this may be a board member, partner or member of Senior Management who must be responsible for the Firm's compliance with the AML regime. The individual should have:
    a. An understanding of the business, its service lines and its clients,
    b. Authority to direct all members of staff (including senior members),
    c. The authority to ensure the Firm's compliance with the regime, and
    d. The time, capacity and resources to fulfil the role.
65. Regulation 34 also requires a Firm to appoint a Nominated Officer or Money Laundering Reporting Officer ("MLRO") and Deputy who must be responsible for receiving internal reports and making external reports to the Financial Reporting Authority ("FRA") about suspicious activity. The individual should have:
    a. Sufficient seniority to enforce his decisions,
    b. The authority to make external reports to FRA without reference to another person, and
    c. The time, capacity and resources to review internal reports and make external reports in a timely manner.

[2] Regulation 57

66. Depending on the size, complexity and services of a firm, these two roles may be combined in a single individual provided that person has sufficient seniority, authority, governance responsibility, time, capacity and resources to do both roles properly. This guidance primarily describes the situation in which one individual fulfils the combined role, referred to in this guidance as the AMLCO/MLRO.
67. If not covered by the AMLCO the role of the MLRO should include responsibility for internal reporting procedures and training on those procedures and recognising suspicious activity.
68. The Firm should ensure that there are sufficient resources to undertake the work associated with the AMLCO/MLRO's role. This should cover normal working, planned and unplanned absences and seasonal or other peaks in work.
69. A Deputy MLRO must be appointed according to the AML Regulations and where the AMLCO and MLRO role are not combined this may be performed by the AMLCO.
70. All AMLCO and MLROs, Deputy MLROS should undertake Continuing Professional Development appropriate to their roles.
71. The AMLCO/MLRO should:
    a. Be involved in ML/TF risk assessments and design of the risk-based approach.
    b. Be the connection between staff, the Board (or equivalent managing body) and the regulator.
    c. Support and coordinate management's focus on ML/TF risks in each individual business area. This involves developing and implementing controls that are appropriate to each business area in turn.
    d. Make recommendations to Board (or equivalent managing body) and take remedial action where controls are ineffective.
    e. Draw attention to the areas in which systems and controls are effective and where improvements could be made.
    f. Receive the results of internal audit or internal/external compliance reviews and communicate these to the board (or equivalent managing body).
    g. Report to the board (or equivalent managing body) at least annually, providing an assessment of the operations and effectiveness of the Firm's AML/CFT systems and controls in a written report. These written reports should be supplemented with regular *ad hoc* meetings or comprehensive management information.

72. If a sole practitioner has no employees, the sole practitioner will act as both AMLCO and MLRO and it need not appoint a Deputy MLRO.

Systems and Controls

73. The AML Regulations require Firms to adopt measures and procedures (see Regulation 5) i.e. internal controls. Even sole practitioners should document these controls to assist in demonstrating the controls to supervisors. Throughout this guidance, reference to controls can be interpreted to include written policies and procedures or systems to mean numerous controls operating together.

Regulation 5, (paraphrased) requires Firms to-	Otherwise known as and description
(a) maintain risk-based procedures for -	
(i) identification and verification;	CLIENT DUE DILIGENCE ("CDD") or "ID+V" Effective customer due diligence measures are the bedrock of AML/CFT requirements and the first line of defence for any Firm. Many Firms already have procedures to help them avoid conflicts of interest and ensure they comply with professional requirements for independence. The requirements of the AML Regulations can either be integrated into these procedures, to form a consolidated approach to taking on a new client or addressed separately. See part IV of the AMLRs.
(ii) monitoring;	CDD monitoring means keeping records up to date and trigger based and periodic consideration of the CDD in light of the developing relationship with the client or a transaction.
(iii) screen employees;	Firms should consider the skills, knowledge, expertise, conduct and integrity of all relevant employees both before, and during the course of, their appointment, proportionate to their role in the firm and the MLTF risks they are likely to encounter. It is important that firms have a mechanism for evidencing AML knowledge for example, a test for which the results are recorded can evidence knowledge and expertise. Similarly, regular recorded ethics training can be useful in assessing integrity.

(iv) record-keeping;	Specific requirements on what records to retain and for how long. See Part VIII AMLRs.
(v) risk and sanctions screening; (vi) risk-management pre-verification;	This forms part of CDD with checks conducted at the same time and as part of ID+V.
(vii) observance of high risk countries;	This forms part of the Risk Assessment and Risk-Based Approach, per Regulation 8
(viii) internal reporting (unless a sole practitioner);	Internal Reporting (suspicious activity). Procedures should clearly set out what is expected of an employee who becomes aware of, or suspects, money laundering, and how they report to the MLRO.
(viiia) ongoing monitoring to prevent counter and report ML, TF and PF and to identify assets subject to TFS,	Procedures will be based on risk assessments of both relationships and transactions and will typically entail periodic screening of clients and real-time screening of payees.
(viiib) to ensure compliance with TFS; and	Procedures will be based on risk assessments of both relationships and transactions and will typically entail periodic screening of clients and real-time screening of payees.
(ix) other internal controls, including an appropriate effective risk-based independent audit function and communication;	AML CFT CFP Audit where the controls and system are assessed and tested periodically.
(b) comply with the identification and record-keeping requirements of Parts IV and VIII;	CDD (ID+V) is to some extent prescribed in Part IV particularly for corporate clients and must be complied with.
(c) make employees aware of – (i) the procedures under paragraph (a); and (ii) the enactments relating to money laundering;	Training to ensure that relevant employees: (a) are aware of their legal and regulatory duties; (b) are continuously updated about changes in the Firm's AML policies, systems and controls,

(d) provide employees with training in the recognition and treatment of suspicious transactions; and	(c) how to recognize suspicious activity, and (d) the ML/TF/PF risks faced.
(e) designate an Anti-Money Laundering Compliance Officer.	As required by Regulation 3.

C. RISK BASED APPROACH

74. Regulation 8 allows and indeed requires Firms to focus resources on the areas of greatest risk, "a risk-based approach" and tailor its response in proportion to its perceptions of risk. This identifies the risks and then applies risk-based controls for CDD and monitoring.

Regulation 8. (1) A person carrying out relevant financial business shall take steps appropriate to the nature and size of the business to identify, assess, and understand its money laundering and terrorist financing risks in relation to -	
(a) a customer of the person;	**"Client Risk"**
(b) the country or geographic area in which the customer under paragraph (a) resides or operates;	**"Country Risk"**
(c) the products, services and transactions of the person; and	**"Service Risk"**
(d) the delivery channels of the person.	**"Delivery Channel Risk"**

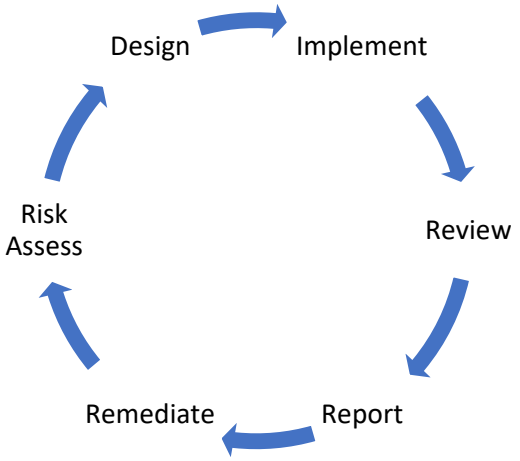
Regulation 8(2) A person carrying out relevant financial business shall -
(a) document the assessments of risk of the person;
(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
(c) keep the assessments of risk of the person current;
(d) maintain appropriate mechanisms to provide assessment of risk information to competent authorities and self-regulatory bodies;

(e) **implement policies, controls and procedures which are approved by senior management, to enable the person to manage and mitigate the risks that have been identified by the country or by the relevant financial business;**
(f) identify and assess the money laundering or terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products;
(g) monitor the implementation of the controls referred to in paragraph (e) and enhance the controls where necessary; and
(h) take enhanced customer due diligence to manage and mitigate the risks where higher risks are identified.

75. The risk-based approach ("RBA") is fundamental and applies to Firms, the Government and AML Supervisors requiring them to analyse the ML/TF risks they face and take proportionate responses to them. A RBA is the foundation of any Firm' AML/CFT procedures.
76. The RBA is underpinned by evidence-based decision-making to better target risks. Controls will never detect and prevent all money laundering, but a realistic analysis of actual risks enables a Firm to concentrate the greatest resources on the greatest threats.
77. The RBA does not exempt low-risk clients, services and situations from AML/CFT procedures, rather procedures can be less onerous than for those thought to present a normal or higher level of risk.
78. The Firm should ensure that ML TF risks are analysed – their nature and severity identified and assessed to produce an accurate risk profile and then act to mitigate those risks in proportion to the severity of the threats they pose.
79. Where a ML TF PF risk is identified, the Firm must design and implement appropriate procedures to manage it. The reasons for believing these procedures to be appropriate should be supported by evidence, documented and systems created to monitor effectiveness.
80. ML TF PF risks include the possibility that the Firm might:
    a. be used to launder money (e.g. by holding criminal proceeds in a client money account or by becoming involved in an arrangement that disguises the beneficial ownership of criminal proceeds);
    b. be used to facilitate money laundering by another person (e.g. by creating a corporate vehicle to be used for money laundering or by introducing a money launderer to another regulated entity);

c. suffer consequential legal, regulatory or reputational damage because a client is involved in money laundering.

81. The risk profile of any Firm changes over time along with the business and its operating environment. The risk analysis should be refreshed regularly, the frequency of which should reflect the ML TF PF risks faced and the stability or otherwise of the business environment. A fresh analysis may then require AML/CFT/CFP procedures to be amended and fed into the review of the System. The Firm may already have general risk analysis processes, and these could form the basis of its ML TF PF risk analysis.



82. Risks are grouped into categories: 'client', 'service', 'geography' and 'delivery channels' but don't look at individual risks in isolation. When two threats are combined they can produce a total risk greater than the sum of the parts.
83. The risk assessment of the Firm should show where particular risks are likely to arise, and so where certain controls will be needed to tackle them.

Client Risk

84. Client risk is the MLTFPF risk posed by a client. The Firm should ask itself "Does our client have attributes known to be frequently used by money launderers or terrorist financiers?"
85. Firms should have different client risk ratings such as: low, normal/medium, and high.
86. The following may suggest a high risk of money laundering or terrorist financing.
    a. Undue client secrecy (e.g. reluctance to provide requested information)
    b. Unnecessarily complex ownership structures (including nominee shareholders or bearer shares);
    c. Underlying Business activities:
        1. cash-based businesses;
        2. money service bureaus;

3. arms dealers;
4. property transactions with unclear source of funds;

d. Resident or national of high risk country (see para 88)
e. politically exposed person;
f. new clients carrying out one-off transactions;
g. rapid rate of turnover (i.e., trades for a short period of time, close down and then starts up as a new company)
h. client is taking on work which is outside its normal range of goods and services;
i. clients that are involved in transactions that don't make commercial sense or involved in transactions where the source of funds is unusual or unknown;
j. high net worth individuals;
k. uncooperative clients;
l. clients who:
    1. have known criminal convictions relating to the proceeds of crime;
    2. are on the sanctions lists (see also para 127)
m. the client's life style and/or transactions are inconsistent with known business and personal information;
n. the client has multiple bank accounts or foreign accounts with no good reason;
o. the client has changed professional advisors a number of times in a short space of time without legitimate reasons,
p. the service being requested was refused by another professional advisor without legitimate reasons, or
q. the customer is prepared to pay substantially higher fees than usual without legitimate reasons.

Service risk

87. Service risk is the perceived risk that certain services present an increased level of vulnerability in being used for MLTF purposes. The Firm should ask itself "Do our services have attributes known to be used by money launderers or terrorist financiers?"
    Services in which there is a serious risk that the Firm itself could commit a money laundering offence should be treated as higher risk.
88. CIIPA has prepared and issued Money Laundering, Terrorist Financing, Proliferation Financing and Targeted Financial Sanctions: Inherent Risk relating to the Accounting Services in the Cayman Islands which should be referred to first but in summary:

Higher Risk Services	Medium Risk Services	Lower Risk Services
Company formation and termination (when offered by accountants)	Fiduciary (e.g. directorships and trustee services)	Audit and Assurance
Accounting and Bookkeeping-False Accounts		Tax Services
Handling Client Money and accounts		
Payroll		
Firms may consider other services as higher risk but where firms wish to classify services as lower risk than as assessed by CIIPA above firms are invited to explain their rationale to CIIPA at the time of the assessment. Note that not all services listed above will constitute 'relevant financial business"		

89. When a Firm decides to have different controls in different parts of the business, it should consider how to deal with clients whose needs straddle departments or functions.
90. Before a Firm begins to offer a service significantly different from its existing range of services, it should reperform the assessment of the MLTF risks and respond appropriately to any new or increased risks. See Regulation 9.

Country risk

91. Country (or Geographic) risk is the increased level of risk that a jurisdiction in connection with services and clients, presents in respect of ML/TF/PF activity.
92. Firms should consider the following sources of information and factors to determine those countries or geographies where money laundering or terrorist financing risk is high:
    a. Subject to embargoes or sanctions by UN or EU,
    b. Countries where individuals and entities are sanctioned for terrorism or country provides funding for terrorism,
    c. Countries identified by Financial Action Task Force as being deficient regarding its recommendations or otherwise are high-risk jurisdictions,
    d. Transparency international perception index,
    e. Cayman's National Risk Assessment 2017, or
    f. Significant part of the economy operates outside the law or a legitimate business infrastructure.

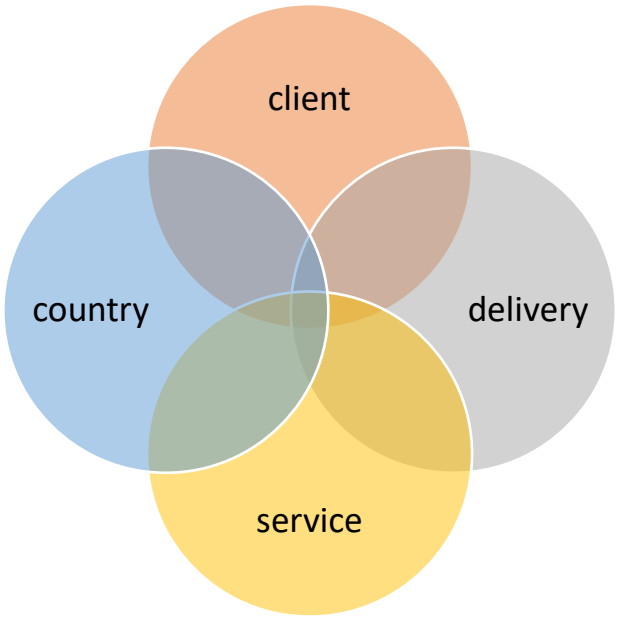
93. The controls used for each category should be suitable for the risks typically found in that category. For example:
    a. If it is normal for a Firm to deal with clients from a high-risk jurisdiction, the Firms' procedures for what they regard as normal clients must be designed to be address the risks associated with the high risk jurisdiction.
    b. If, a firm has no experience of a particular country, it could treat it as a normal or high risk even though other Firms might consider it low risk.
    c. If a Firm expects to deal with only Cayman Islands individuals and entities, it may treat as high risk any client associated with a non-Cayman Islands jurisdiction.

Delivery channel risk

94. Certain delivery channels can increase the MLTF risk, because they can make it more difficult to perform CDD for a client or to monitor the relationship
95. For example, delivery channel risk could be increased where services / products are provided to clients who have not been met face to face, or where a business relationship with a client is conducted through an intermediary. This in turn is affected by the role and degree of control of the intermediary, the location and any restrictions on access to information/data.

Combining and Comparing Risks

96. The various risks may be weighted and should also be considered in combination with each other. Delivery Risk may not be applicable and service risks do not need to be differentiated if the Firm only provides one service.
97. Firms should be able to demonstrate to CIIPA how they assess and seek to mitigate ML TF PF risks. This assessment should be documented and made available to CIIPA



on request. The documentation should demonstrate how the risk assessment informs their controls. (see Regulation 53A)

98. The combination of Client and Service Risk might be illustrated as follows depending on the weighting assigned:

		Services Risk		
Client Risk		Low	Medium	High
	Low			
	Med			
	High			

D. CUSTOMER DUE DILIGENCE & MONITORING

99. The purpose of Customer Due Diligence ("CDD") is to know and understand a client's identity and business activities so that any money laundering or terrorist financing risks can be properly detected. Effective CDD is, therefore, a key part of AML/CFT/CFP controls. By knowing the identity of a client, including who has ultimate ownership and control, a Firm not only fulfils its legal and regulatory requirements, but it equips itself to make informed decisions about the client's professional standing and acceptability and therefore the risk.

100. CDD also helps a Firm to construct a better understanding of its typical client profile. By understanding normal practice, it is easier to detect abnormal events, which, in turn, may point to money laundering or terrorist financing activity.

Regulation 11: A person carrying out relevant financial business shall undertake customer due diligence measures when -
(a) establishing a business relationship;
(b) carrying out a one-off transaction valued in excess of ten thousand dollars, including a transaction carried out in a single operation or in several operations of smaller value that appear to be linked;
(c) carrying out a one-off transaction that is a wire transfer;

(d) there is a suspicion of money laundering or terrorist financing;[3] or
(e) the person has doubts about the veracity or adequacy of previously obtained customer identification data.[4]

101. Where its services are relevant financial business the Firm must ensure that customer due diligence is applied to new and existing clients alike. For existing clients, CDD information gathered previously should be reviewed and updated where it is necessary, timely and risk-appropriate to do so.

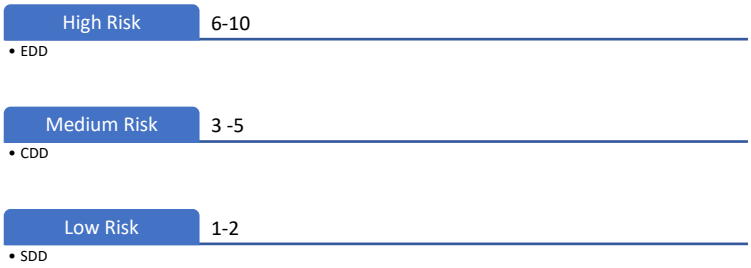
12. (1) A person carrying out relevant financial business shall -	
(a) identify a customer, whether a customer in an established business relationship or a one-off transaction, and whether natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information;	In short this means ID + V Where ID = identify the client by obtaining information, (often from the client) about the client (see para 106) And where V = Verify the information provided by obtaining proof (see para 108)
(b) verify that a person purporting to act on behalf of a customer is properly authorised and identify and verify the identity of the person;	
(c) identify a beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from reliable sources, so as to be satisfied that the person knows the identity of the beneficial owner;	
(d) understand and obtain information on, the purpose and intended nature of a business relationship; and	This information is obtained from the client and is not usually verified but is monitored once the relationship is established.
(e) conduct **ongoing due diligence** on a business relationship including -	
(i) scrutinising transactions undertaken throughout the course of the business	"Trigger based Monitoring" (see para 133)

[3] Where there is such knowledge or suspicion the Firm needs to consider not only whether the existing CDD information is sufficient and up-to-date, but also whether a suspicious activity report (SAR) should be made to the FRA.

[4] CDD procedures must also be carried out at certain other times, such as when there is a suspicion of money laundering or terrorist financing, or where there are doubts about the available identity information, perhaps following a change in ownership/control or through the participation of a politically exposed person, or PEP.

	relationship to ensure that transactions being conducted are consistent with the person's knowledge of the customer, the customer's business and risk profile, including where necessary, the customer's source of funds; and	Transaction includes financial transactions, and instructions or changes.
	(ii) ensuring that documents, data or information collected under the customer due diligence process is kept current and relevant to customer due diligence, by reviewing existing records at **appropriate times**, taking into account whether and when customer due diligence measures have been previously undertaken, particularly for higher risk categories of customers.	"Periodic Monitoring" (see para 135) What is an appropriate time depends on risk .

102. While the AML Regulations prescribe the level of CDD that should be applied in certain situations (i.e. simplified or enhanced), they do not describe how to do this on a risk-sensitive basis. The Firm should be able to demonstrate to CIIPA that the measures it applied were appropriate. Whilst a Firm may simply adopt High-Medium-Low categories one method to further demonstrate a risk-based approach is to consider risk on a scale of 1-10, where:



103. Customer due diligence should be completed **before** entering into a business relationship or undertaking a one-off transaction, unless Regulation 15(2) applies.

Regulation 2 "business relationship" means any arrangement between two or more persons where -
(a) the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent, habitual or regular basis; and
(b) the total amount of any payment or payments to be made by any person to any other in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made.

104. Thus, generic advice, provided with no expectation of any customer follow-up or continuing relationship (such as generic reports provided free of charge or available or purchased by anyone), is unlikely to constitute a business relationship (although may potentially be a one-off transaction).

> "one-off transaction" means any transaction other than a transaction carried out in the course of an established business relationship formed by a person carrying out relevant financial business;

105. For a one-off transaction to be relevant financial business requiring CDD it must have a value of $10,000 or more. If the client returns for another service, then this may constitute a business relationship.

Identification ("ID")

106. The **identification** phase requires the gathering of information about a client's identity and the purpose of the intended business relationship. Minimum identification information for an individual is:
    a. full name,
    b. date of birth,
    c. nationality, and
    d. residential address.

107. This can be collected from a range of sources, including the client but exercise caution in higher risk cases. In the case of corporate clients and other organisations, identification also extends to establishing the identity of anyone who ultimately owns or controls the client. These people are the 'beneficial owners' ("BenOs").

Verification ("V")

108. Once an initial risk assessment has been carried out, evidence from an independent, reliable source is required to verify the identity information gathered. This is called **verification**. Whilst the initial risk assessment may highlight a need for more information to be gathered or a fresh risk assessment performed, note that the client risk assessment is continual and will require review especially during verification and monitoring. For this reason, it is not usually effective to take a "tick box" approach to CDD and monitoring.

15. (1) A person carrying out relevant financial business shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for one off customers.

109. Client verification means to verify on the basis of documents or information obtained from a reliable source which is independent of the person whose identity is being verified. Documents issued or made available by an official body can be regarded as being independent of a person even if they are provided or made available by or on behalf of that person.
110. The AML Regulations do not prescribe what information sources a Firm should consult for verification. There are many possibilities, including collecting information from websites, brochures and reports, as well as public domain sources. Since the purpose of client verification is to check the client identity information already gathered, it is important that the information used at this stage is drawn from independent sources.
111. Enhanced Due Diligence ("EDD") might include more extensive internet and media searches covering the client, key counterparties, the business sectors and jurisdictions. Subscription databases can be a quick way to access this kind of public domain information, and they will often reveal links to Family members and Close Associates of Politically Exposed Persons ("PEPS").

Beneficial ownership

112. A Beneficial Owner can only be a living breathing 'natural' person (unless a trust, see para **CDD for Trusts and other legal arrangements**).
113. Regulation 2 of the AML Regulations defines the meaning of 'beneficial owner' for a range of different client types. There may be situations in which someone is considered to be the beneficial owner by virtue of control even though their ownership share is less than 10%.

"beneficial owner" means the natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted and includes but is not restricted to -
(a) in the case of a legal person other than a company whose securities are listed on a recognised stock exchange, a natural person who ultimately owns or controls, whether through direct or indirect ownership or control, **10%** or more of the shares or voting rights in the legal person;
(b) in the case of any legal person, a natural person who otherwise exercises **ultimate effective control** over the management of the legal person; or
(c) in the case of a legal arrangement, the trustee or other person who exercises **ultimate effective control** over the legal arrangement;…

114. Firms need to be diligent in their enquiries about beneficial ownership, taking into account that the information they need may not always be readily available from public sources. A flexible approach to information gathering will be needed as it will often involve direct enquiries with clients and their advisers as well as searches of public records.
115. In many situations determining beneficial ownership is a straightforward matter unless the client is part of a complex structure which in itself may result in a high-risk rating.

CDD for Individuals

Risk	Identification
All	Full name, Date of birth Residential address Nationality
Risk	**Verification**
Normal risk CDD	The original, or an **acceptably certified**[5] copy, of one of the following documents should be seen and a copy retained: • valid passport • valid photo card driving licence • national Identity card (non-Cayman Islands nationals)
High risk EDD	**In addition to the above** The original of a second document should be seen and a copy retained. This should be one of the following: • A valid full Cayman Islands driving licence. • Recent evidence of entitlement to a state- or local authority-funded benefit • Instrument of a court appointment (such as a liquidator or grant of probate). • Government issued tax notification. • Current bank statements or credit/debit card statements (including electronic if evident issued in that form). • Current utility bill.

[5] See para 35

	Source of wealth and source of funds At a minimum search and record from public online information including, company and land registers and depending on risk obtain originals or certified copies of: • Audited financial statements • Bank statements • Proof of property sale • Proof of inheritance • Proof of business sale

CDD for Companies

Risk	Identification
All	• full name of company • registered office address and, if different, principal place of business • any shareholders/members who ultimately own or control more than 10% of the shares or voting rights (directly or indirectly), or any individual who otherwise exercises control over management any agent or intermediary purporting to act on behalf of the entity e.g. where a lawyer engages on behalf of an underlying client
Risk	**Verification**
Normal risk CDD	The original, or an **acceptably certified** copy, of one of the following documents should be seen and a copy retained: • Certificate of incorporation • Memorandum and Articles of Association • Register of Members • Register of Directors and Officers
High risk EDD	**In addition to the above** • Letter of good standing • Audited financial statements or management accounts if not audited

CDD for Trusts and other legal arrangements

See Regulation 12(2)

Risk	Identification
All	Full name, date of birth and address of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control or ownership);
Risk	**Verification**
Normal risk CDD	• Trust deed • As for individuals and companies above
High risk EDD	• As for individuals and companies above • Confirmation of professional or regulated status of the person forming the trust

Risk-based CDD

116. This is important, not only to ensure that there is good depth of knowledge in higher risk cases, but also to avoid disproportionate effort in lower risk cases.

Simplified due diligence (SDD)

117. Simplified due diligence can be applied in a low risk case as prescribed in Regulation 22 where client is:

(i) required to comply with regulation 5 or is a majority owned subsidiary of the relevant financial business;

(ii) a central or local government organisation, statutory body or agency of government, in a country specified in the list published by the Anti-Money Laundering Steering Group;

(iii) acting in the course of a business or is a majority-owned subsidiary of the business in relation to which an overseas regulatory authority exercises regulatory functions and is based or incorporated in, or formed under the law of, a country specified in the list published by the Anti-Money Laundering Steering Group;

(iv) a company, that is listed on a recognised stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, or majority-owned subsidiary of such a company; or

(v) a pension fund for a professional association, trade union or is acting on behalf of employees of an entity referred to in sub-paragraphs (i) to (iv).

118. Customer **Identification** is still required but the extent and timing of **verification** and the degree of reliance placed on others if applicable, may be adjusted to reflect the assessment of low risk.

Identification must include a print-out from the website of the regulator or stock exchange or government website and in the case of any doubts or possible negative factors, written confirmation from the relevant regulator or stock exchange should be requested and obtained. Ongoing monitoring for unusual or suspicious transactions is still required and this may be simplified compared to what is done for normal risk, but it is often easier to adopt the same approach to monitoring for both normal and low risk.

119. The Firm's internal procedures should set out clearly what constitutes reasonable grounds for a client to qualify for SDD and must take into account at least the risk factors and this guidance.

120. In any case, when a client or potential client has been subjected to SDD, and a suspicion of money laundering or terrorist financing arises nonetheless, appropriate (i.e. normal or enhanced) due diligence procedures applied instead (with due regard given to any risk of tipping off).

Enhanced due diligence (EDD)

Regulation 27. Subject to regulation 19, a person carrying out relevant financial business shall perform enhanced customer due diligence -
(a) where a higher risk of money laundering or terrorist financing has been identified pursuant to Part III;
(b) where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;
(c) where a customer or an applicant for business is from a foreign country that has been identified by credible sources as having serious deficiencies in its anti-money laundering or counter terrorist financing regime or a prevalence of corruption;
(d) in relation to correspondent banking relationships, pursuant to Part XI;
(e) where the customer or the applicant for business is a political exposed person; or
(f) in the event of any unusual or suspicious activity.

121. EDD procedures may include one or more of the following—

a. seeking additional independent, reliable sources to verify information provided to the Firm;

b. taking additional measures to understand better the background, ownership and financial situation of the client, and other parties to the transaction;

c. taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;

d. Increasing the monitoring of the business relationship, including greater scrutiny of transactions.

Politically exposed persons

122. Politically exposed persons ("PEPS") including their family and any associated persons, companies or other organisations ("Close Associates") pose higher money laundering risks because their positions can make them vulnerable to corruption. It is important to identify PEPs so that the Firm can properly consider the risks associated with any engagement involving them and apply EDD.

30. (1) A person carrying out relevant financial business shall in addition to satisfying customer due diligence requirement shall under these Regulations -	
(a) put in place risk management systems to determine whether a person or beneficial owner with whom that person has a business relationship is a politically exposed person, family member or close associate;	The system should be risk based largely in terms of the method to check and how often to screen or check during the relationship. Some Firms may subscribe to commercial systems that have recorded PEPs, family members and close associates and Firms likely to provide services regularly to PEPs should consider subscribing. If not more information may be needed on family and associates so the Firm can check if they are PEPs. Determining close associates of PEPs is particularly difficult if not subscribing to a commercial system. Firms should use risk-sensitive measures to help them to recognise PEPs. This can be as simple as asking the client themselves or searching the internet. During the life of a relationship reasonable steps should be taken to keep abreast of developments that could transform an existing client into a PEP.
(b) ensure that the risk management procedures under subparagraph (a) -	
(i) contain as a component, procedures for requiring that senior management approval be obtained before establishing or continuing a business relationship with a politically exposed person or a family member or close associate;	
(ii) take reasonable measures to establish the source of wealth and the source of funds of a person involved in a business relationship and a beneficial owner identified as a politically exposed person or a family member or close associate; and	Source of Funds is the source or origin from which funds may be received for fees or if handling transactions, funds. Source of Wealth is how the person acquired wealth or funds for example employment, property development and other business interests. The earnings from a political career do not usually result in significant wealth. Being in business prior to political career may have generated significant wealth which in many countries should all be disclosed and divested. Extensive checks are required where a client is a PEP to ensure that the funds are not the proceeds of corruption or other illegitimate activity.

(iii) contain as a component, monitoring of the business relationship with the politically exposed person or a family member or close associate.	

123. In cases where a client (an individual) or beneficial owner of a client is identified as a PEP, an enhanced level of due diligence must be performed on the PEP. Firms should also undertake an increased level of monitoring in respect of the client relationship, although a risk based approach may determine that this is not necessary as PEPs do vary in risk as does the degree of initial CDD performed and recorded.
124. Firms should determine that an individual is no longer a PEPs no less than 12 months after they resign from the position. Where PEPs are removed from office Firms should consider the person to be high risk until the reason for removal is made known or proven. This does not apply to family members or known close associates.
125. In higher risk cases however, Firms should continue to treat individuals as PEPs after they cease to hold the position and extend the requirements to family members and known close associates of PEPs.

Targeted Financial Sanctions

126. Firms must comply with any sanctions, embargos or restrictions in respect of any person or state to which the UN, EU UK or Cayman has decided to apply such measures (a list is published by HM Treasury). Firms may be directed to not enter into business relationships, carry out one-off transactions or proceed with any arrangements already in progress. Depending on the circumstances, sanctions imposed by the US may also apply to Cayman Islands Firms.
127. HM Treasury publishes guidance to assist firms and the Financial Reporting Authority of the Cayman Islands has also issued guidance (go to www.fra.gov.ky).
128. CIIPA communicates changes to the list of sanctioned persons and entities by email to the AMLCO of each registered firm. Upon receipt of a notice of a change, if the change entails an addition or a change to information regarding sanctioned persons or entities:
    a. if a firm is using a commercial database which does not run daily screening, it should ensure screening is conducted,
    b. if the firm does not have a commercial database and screens against the list of sanctioned persons and entities manually, then it should conduct a manual screen.

129. Once a person or entity is identified as subject to sanctions the firm must cease providing services and/or freeze assets and report without delay in accordance with the various Sanctions Orders. For more information see various resources at www.fra.gov.ky.

Originals and Acceptably Certified Copies for Verification

Certification

130. Firms should consider how they will demonstrate the reliability of document copies. When the original was seen by an employee it should be sufficient for that person to endorse the copy to that effect, including the date on which it was seen, provided they have received training in that regard or are a member of senior management and there should be controls to this effect.
131. When the copy originates from outside the business, Firms should restrict acceptance to certification by notaries, lawyers and professional accountants or similar independent, competent persons subject to ethical requirements.

Timing and Incomplete CDD

132. The AML Regulations recognise that **verification** will sometimes need to be completed while the business relationship is established, rather than before.

Regulation 15(2) If permitted by these Regulations, the person may complete verification after the establishment of the business relationship, provided that -
(a) this occurs as soon as reasonably practicable;
(b) this is essential not to interrupt the normal conduct of business; and
(c) the money laundering or terrorist financing risks are effectively managed.

133. In some situations, it may be necessary to carry out verification while commencing work because it is urgent. Examples include:

    a. some insolvency appointments;

    b. appointments that involve ascertaining the client's legal position or defending them in legal proceedings;

    c. response to an urgent cyber incident;

d. when it is critically important to preserve or extract data or other assets without delay.

134. When most of the information needed has been collected before the business relationship has begun, it may be acceptable to have a short extension (to allow for information collection to be completed) provided:
    a. the cause of the delay is administrative or logistical, not the client's reluctance to cooperate,
    b. the reasons are valid and do not give rise to suspicions of money laundering,
    c. each extension should be subject to risk based controls, considered individually and agreed by senior management,
    d. extensions should be specific, well-defined and time-limited,
    e. there should be no granting of general extensions (such as for particular client types), and
    f. no client assignments (including transfers of client money or assets) should be completed until verification has been completed in accordance with the Firm's own procedures.

On-going monitoring of the client relationship

Trigger-based Monitoring

135. Firms need to make sure that documentation, data and information obtained for CDD purposes is kept up-to-date. Events prompting a CDD update should include:
    a. a change in the client's identity information
    b. a change in beneficial ownership or control of the client
    c. a change in the service provided to the client
    d. information is obtained that is inconsistent with the Firm' knowledge of the client
    e. change in the risk or factors affecting the risk rating

136. A review may also be triggered by:
    a. the start of a new engagement;
    b. planning for recurring engagements;
    c. a previously stalled engagement restarting;
    d. a significant change to key office holders;

e. the participation of a PEP;

f. a significant change in the client's business activity (this would include new operations in new jurisdictions); and

g. there is knowledge, suspicion or cause for concern (for example where you doubt the veracity of information provided). If a SAR has been made, care must also be taken to avoid making any disclosures which could constitute *tipping off*).

Periodic Monitoring

137. Firms should also conduct periodic reviews to update their CDD. The frequency of up-dating should be risk-based, reflecting the Firm's knowledge of the client and any changes in its circumstances or the services it requires.

As an example:

Low Risk	1-3 years
Medium Risk	6 months to a year
High Risk	Every month or quarter

138. The CDD procedures required for either Trigger-driven or Periodic reviews may not be the same as when first establishing a new business relationship. Given how much existing information could already be held, on-going CDD may require the collection of less new information than was required at the very outset.

Cessation of work and suspicious activity reporting

139. If a prospective or existing client refuses to provide CDD information, the work must not proceed and any existing relationship with the client must be terminated.

Regulation 18. Where a person carrying out relevant financial business is unable to obtain information required by these Regulations to satisfy relevant customer due diligence measures -
(a) the person shall -
(i) not open the account, commence business relations or perform the transaction; or
(ii) terminate the business relationship; and
(b) the person shall consider making a suspicious activity report in relation to the customer.

Further

Regulation 19. Where a person carrying out relevant financial business	
(a) forms a suspicion of money laundering or terrorist financing; and	See para 45
(b) reasonably believes that satisfying ongoing customer due diligence requirements of these Regulations for a customer or customer due diligence requirements of these Regulations for an applicant for business will tip-off a customer or an applicant for business,	
the person shall not complete the customer due diligence requirements of these Regulations but shall file a suspicious activity report.	

E. SUSPICIOUS ACTIVITY REPORTING (Internal Reporting)

140. It is an offence for someone who knows or suspects that money laundering has taken place (or has reasonable grounds) and not report their concerns to their MLRO (or to the FRA).
141. According to the AML Regulations, Firms conducting relevant financial business must have internal reporting procedures that enable staff to disclose their knowledge or suspicions of money laundering or terrorist financing and a MLRO must be appointed to receive these disclosures.
142. As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction, but for an established client, a suspicious transaction will often be one which is inconsistent with that client's known, legitimate business or personal activities. Therefore, the first key to recognition is knowing enough about the client and the client's business to recognise that a transaction, or series of transactions, is unusual. Such transactions may arise at any stage, and commonly occur within an established relationship rather than at the outset.
143. Warning signs which can indicate that an established client's transaction might be suspicious include:
    a. the size of the transaction (or transactions when aggregated) is inconsistent with the normal activities of the client;

b. the transaction is not rational in the context of the client's business or personal activities;
c. the pattern of transactions conducted by the client has changed;
d. the client has no obvious reason for conducting business with a country involved in the transaction.

144. The type of situations giving rise to suspicion will depend on a firm's client base and range of services. Sufficient direction must be given to partners and staff to enable them to recognise suspicious transactions. Firms might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports, with a view to updating internal controls from time to time.

Liability of Firms

145. Section 142 of the POCL may impose liability on firms, regardless of whether they carry on relevant financial business or not, to report suspicions of money laundering related to conduct through vicarious liability.
146. All firms thus have a clear obligation to ensure:
    a. that each relevant partner and member of staff knows to which person he or she should report suspicions; and
    b. that there is a clear reporting chain under which those suspicions will be passed without delay to the MLRO.
147. Once an employee has reported his/her suspicions to the MLRO, he/she has fully satisfied the statutory obligation but see para 48.

Internal reporting controls

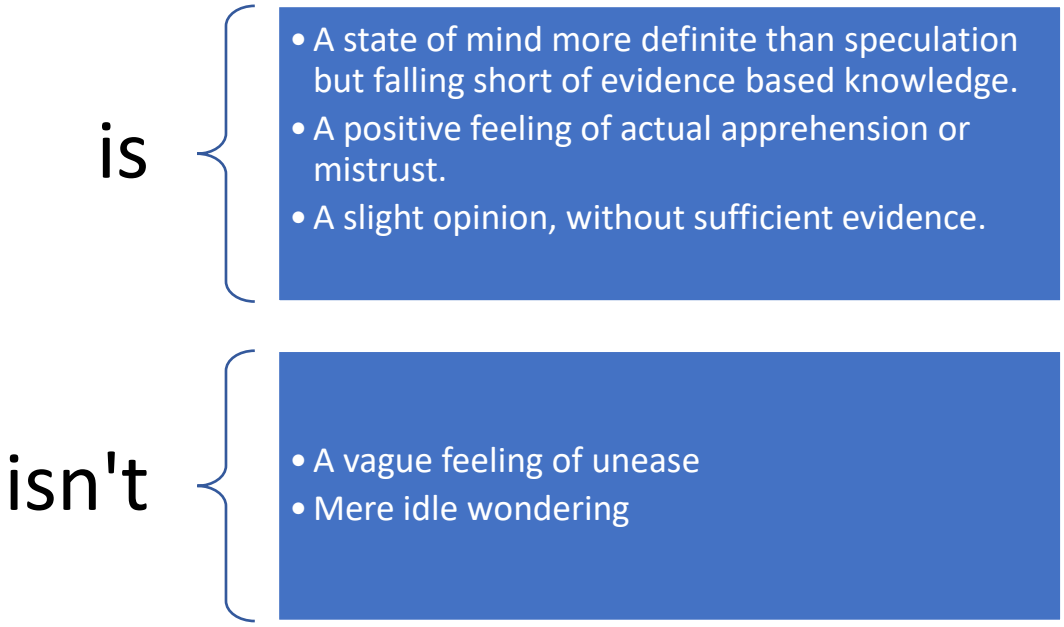
148. Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO. However, some firms may choose to require that unusual or suspicious transactions be drawn initially to the attention of an appropriate partner to ensure that there are no known facts that will negate the suspicion before further reporting to the MLRO.
149. Such partners should also be aware of their own legal obligations. An additional fact which the partner supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the partner. The firm's procedures should then require the partner to report to the MLRO. On the other hand, the partner should never attempt to prevent a member

of staff who remains suspicious from reporting direct to the MLRO. Staff should be made aware that they have a direct route to the MLRO.

150. All procedures and responsibilities in should be documented in appropriate manuals and job descriptions where necessary. There is no POCL-compliant format prescribed for internal reports to an MLRO so Firms should devise their own.

151. All suspicions reported to the MLRO should be documented (in urgent cases this may follow an initial discussion by telephone). In some firms it may be possible for the person with the suspicion to discuss it with the MLRO and for the report to be prepared jointly. In other firms the initial report should be prepared and sent to the MLRO. The report should include full details of the client and as full a statement as possible of the information giving rise to the suspicion.

152. What constitutes 'suspicion' remains subjective. Some pointers can be found in case law, where the following observations have been made about what suspicion does and doesn't feel like:



153. A report must be made where there is knowledge or suspicion of money laundering, but there is no requirement to make speculative reports, e.g.

    a. a suspicion is formed that someone has failed to declare all of their income for the last tax year, to assume that they had done the same thing in previous years would be speculation in the absence of specific supporting information.

b. the purchase of a brand new Ferrari by a client's financial controller is not, in itself, suspicious activity. However, inconsistencies in accounts for which the financial controller is responsible could raise speculation to the level of suspicion.

154. A report is also required when there are 'reasonable grounds' to know or suspect. This is an objective test; i.e. the standard of behaviour expected of a reasonable person in the same position. Claims of ignorance or naivety are no defence.

155. It is important for individuals to make enquiries that would reasonably be expected of someone with their qualifications, experience and expertise, and as long as they fall within the normal scope of the engagement or client relationship. In other words, they should exercise professional skepticism and judgement and, if unsure about what to do, consult their MLRO (or similar) in accordance with the business's own procedures. If in doubt, err on the side of caution and report to the MLRO.

156. The information or knowledge that gave rise to the suspicions must have come to the individual in the course of business.

157. In most cases of suspicious activity, the reporter will have a particular type of criminal conduct in mind, but this is not always the case. Some transactions or activities so lack a commercial rationale or business purpose that they give rise to a general suspicion of money laundering.

158. It is important that documents containing references to the subject matter of any AML report are not released to third parties without first consulting the MLRO and, in extreme cases, law enforcement. Examples of such documents include:

    a. public audit or other attestation reports;

    b. public reports to regulators;

    c. confidential reports to regulators;

    d. professional clearance/etiquette letters;

    e. communications to clients of an intention to resign.

159. When more than one individual is aware of the same reportable matter a single report can be submitted to the MLRO, but it should contain the names of all those making the report.

Onward reports by the MLRO to the FRA

160. The MRLO has a duty to consider all such reports. If the MLRO also suspects money laundering then a suspicious activity report ("SAR") must be made to the FRA.

161. The MLRO should acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. to avoid "tipping off".
162. Often, the MLRO's knowledge or suspicions will arise (directly or indirectly) out of the internal reports they receive. In making this judgement, the MLRO should consider all other relevant information available within the firm concerning the person or business to whom the initial report relates. This may include making a review of other transaction patterns and volumes, the length of the business relationship, and referral to identification records held. MLROs sometimes need advice when formulating instructions to the wider business. Legal advice can be sought from a suitably skilled and knowledgeable professional legal adviser. Discussion with the FRA and law enforcement may also be valuable but bear in mind that they cannot provide advice and they are not entitled to dictate the conduct of a professional relationship.
163. If after completing this review, he/she knows or suspects that any person is engaged in money laundering, then he/she must ensure that the information is disclosed to the FRA.
164. Nevertheless, care should be taken to guard against a report being submitted as a matter of routine to the FRA without undertaking reasonable internal enquiries to determine that all available information has been taken into account.
165. Regulation 34 refers to the MLRO "determining" whether or not the information or other matter contained in the report does give rise to a knowledge or suspicion that a person is engaged in money laundering. This implies a process with some formality attached to it. The MLRO will be expected to act honestly and reasonably and to make his/her determinations in good faith. Providing the MLRO or an authorised deputy does act in good faith in deciding not to pass on any suspicions report, there will be no liability for non-reporting if the judgment is later found to be wrong, although it should be borne in mind that in the vast majority of cases the determination will only be scrutinised after the event when it has turned out to be wrong. Consequently, in cases of doubt the safer course for an MLRO will be to make a report. The MLRO may also find it prudent to seek legal advice.
166. The MLRO may want to make reasonable enquiries of other individuals and systems within the Firm. These may confirm the suspicion, but they may also eliminate it, enabling the matter to be closed without the need for a SAR.
167. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the FRA, should be documented. This information may be required to supplement the initial report or as evidence of good practice and due diligence if, at some future date, there is an investigation and the suspicions are confirmed.
168. Suspicious activity disclosure should be sent directly to the FRA at the following address:

The Reporting Authority

P.O. Box 1054

George Town, Grand Cayman Telephone: (345) 945-6267

Facsimile: (345) 945-6268

169. There is a prescribed format for an onward report to the FRA.
170. Disclosures can be forwarded by hand, post or by facsimile message. In urgent cases an initial telephone report can be made and confirmed in writing.
171. The receipt of a disclosure should be acknowledged by the FRA. If the acknowledgement is not received promptly, firms should contact the FRA. A further report will be needed if any other transactions give rise to suspicions, or if there are new suspicions concerning a transaction which has already been reported.
172. Sufficient information should be disclosed which indicates the nature of and **reason for the suspicion**. If a particular offence is suspected, this should be stated. Where the firm has additional relevant evidence that could be made available, the nature of this evidence might be indicated to enable the Reporting Authority to obtain a production order if necessary.

What information should be included in a SAR?

173. All reports should be free of jargon and written in plain English. It is very important to set out all the information that has led to the person forming a suspicion including to note what information it considers to be missing.
174. It is also recommended that reporters:

    a. do not include confidential information not required by POCL;

    b. show the name of the business, individual or MLRO submitting the report only once, in Section 1 Reporting Entity Details and nowhere else;

    c. do not include the names of the people who made the internal reports to the MLRO;

    d. include other parties as 'subjects' only when the information is necessary for an understanding of the report or to meet required disclosure standards; and

    e. highlight clearly any particular concerns the reporter might have about safety (whether physical, reputational or other). Put this information in the 'reasons for suspicion/disclosure' field.

175. The Tipping Off offence is not likely to be committed when enquiries are made of a client regarding something that properly falls within the normal scope of the engagement or relationship. So, for example, if a *Firm or individual* discovers an invoice that has not been included on a client's tax return, then the client should be asked about it. Although normal commercial enquiries (perhaps to understand a particular transaction) would not generally lead to tipping off, care is required nonetheless. Enquiries should be confined to what is required by the ordinary course of business. No attempt should be made to investigate matters unless to do so is within the scope of the professional work commissioned. It is important to avoid making accusations or suggesting that anyone is guilty of an offence.
176. The tipping off provisions do not prevent a firm from communicating money laundering suspicions to a client's senior management, internal auditors, or other person responsible for monitoring or reporting money laundering in accordance with professional standards for example IESBA Code of Ethics. However, considerable care is always needed to ensure that there is no inadvertent tipping off and for that reason the firm's MLRO should always be consulted before any such communication is made by the appropriate individual of a senior level of the firm. The MLRO will need to be satisfied
    a. that the persons to whom the firm is reporting its suspicions are not in any way implicated in the money laundering, and
    b. that the information that it is communicating will not be passed to others, so as to risk any investigation or proposed investigation being prejudiced.
177. Where it is known or suspected that a suspicious transaction report has already been made to the FRA and it becomes necessary to make further enquiries, great care should be taken to ensure that clients do not become aware that their names have been brought to the attention of the FRA. There may be occasions where it is feasible for the firm to agree a joint strategy with the FRA to ensure that the interests of both parties are taken into account.

Reporting declined business

178. It is normal practice for many firms to turn away business that they suspect might be criminal in intent or origin. While this is commendable, the firms should give consideration as to whether they are obliged in such circumstances to make a report, albeit that no transaction has taken place.
179. Reporting of such events will allow the FRA to build a clearer picture of the money laundering threat to the Island, and to use such intelligence on a proactive basis. Furthermore, firms should refrain from referring such business to others.

Termination of a business relationship following a disclosure

180. It is not intended to over-ride normal commercial judgement; and a firm is not committed to continuing the relationship with the client if such action would place the reporting firm at commercial or professional risk. However, it is recommended that before terminating a relationship, the reporting firm should liaise with the FRA to ensure that the termination does not "tip-off" the client or prejudice the investigation in any other way. In some more complex situations, firms may wish to take legal advice as to whether termination could have breach of contract implications. (see also para 134)

Reporting to the Police

181. MLROs should distinguish between the making of SAR and the lodging of a complaint or allegation of crime with the police for investigation. For example, a fraudulent deception targeted on third parties, and based on forged documents ostensibly issued by or naming the firm, may not be a matter for a SAR. It may instead be reported as an allegation of crime in the public interest.

Constructive trust

182. A firm's liability as a constructive trustee may arise when it comes to know that assets rightfully belong to a person other than its client. The firm then may take on the obligation of constructive trustee for the true owner. If the assets are dealt with in a way which is inconsistent with the rights of the true owner, the civil law treats the firm as though it were a trustee for the assets and holds the firm liable to make good the loss suffered. Having a suspicion which it considers necessary to report under POCL could be taken as indicating that it knows or should know that the assets belong to a third party.
183. In the normal course of events, a firm would not dispose of assets to a third party knowing itself to be in breach of trust. The concern in relation to money laundering is that the firm will have reported its suspicion to the FRA. It will therefore have no option but to act on the client's instruction, because by refusing to hand over the assets it might alert the perpetrator of, for example a fraud, and in doing so commit a tipping off offence under POCL.
184. Given the absolute nature of the prohibition in the criminal law, if a firm makes a disclosure under POCL, the risk of the firm being held liable by a civil court as constructive trustee is "slight". However, it is suggested that legal advice should be sought.

Confidentiality

185. A correctly made SAR provides full immunity from action for any form of breach of confidentiality, whether it arises out of professional ethical requirements or a legal duty created by contract (e.g. a non-disclosure agreement). There will be no such immunity if the SAR is not based on knowledge or suspicion.
186. Firms may wish to include in their client agreements, terms of business or engagement letters a passage which places clients on notice of the firm's potential reporting obligations. While this could refer specifically to suspicions of money laundering, firms may prefer a generalised form of wording which would extend to other matters where reporting to regulators is required or appropriate. It is also a useful precaution to include a statement that Cayman law will govern the provision of the firm's services and that the Cayman courts will have exclusive jurisdiction over any dispute.
187. A client's new adviser may request copies of identification evidence to help in its own identification procedures. Firms should not release confidential information without the client's consent.

Documenting reporting decisions

188. In order to control legal and regulatory risk, it is important that adequate records of internal reports are kept and those firms engaging in relevant financial business must maintain records according to the AML Regulations. This is usually done by the MLRO and should include details of:

    a. all internal reports made and date;
    b. key reason for suspicion
    c. how the MLRO handled matters, including any requests for further information;
    d. assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek extra information;
    e. the date of the SAR submission to FRA if applicable;
    f. the rationale for deciding whether or not to make a SAR;
    g. any advice given to engagement teams about continued working
    h. the person who made the report; and
    i. a reference by which supporting evidence is identifiable.

189. These records can be simple or sophisticated, depending on the size of the Firm and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. They are important because they may be needed later if the MLRO or some other person is required to justify and defend their actions.
190. For the MLRO's efficiency and ease of reference, a reporting log may assign internal reports a unique reference number.

Reporting and the privileged circumstances exemption

191. Whilst the POCL refers to relevant professional adviser, being an accountant, auditor or tax adviser who is a member of a professional body which tests competence and imposes professional and ethical standards and imposes sanctions for non-compliance, which CIIPA members would be, its relevance is to certain defences based on privileged circumstances, and whether or not the privilege reporting exemption applies to a given situation is a matter for careful consideration. The adviser may have been providing the client with a variety of services, not all of which would create the circumstances required for the exemption.
192. Consequently, it is strongly recommended that careful records are kept about the provenance of the information under consideration when decisions of this kind are being made and legal advice may be needed.
193. Audit work, book-keeping, preparation of accounts or tax compliance assignments are unlikely to take place in privileged circumstances.

Production orders, further information orders and other requests for information

194. The FRA or other law enforcement authority may seek further information about a SAR (usually via the MLRO). Firms should have in place controls to enable a full and rapid response to such enquiries, and any enquiries from law enforcement regarding a business relationship. It is recommended that the enquirer's identity is formally verified before a response is provided. This can most easily be done by noting the caller's name and agency/force and then calling them back through their main switchboard.
195. To the extent that the request is simply to clarify the contents of a SAR, a response can be given without further formalities. It is reasonable for an MLRO to answer questions from an FRA officer or other law enforcement officer aimed at clarifying the content of a SAR. Firms should manage their legal risk accordingly, only making further disclosure to the FRA, law enforcement or prosecuting agencies in response to the exercise of a statutory power to obtain information (as contained in the relevant legislation) or in line with professional guidance on confidentiality

and disclosures in the public interest. This approach protects the MLRO and the business from allegations of breach of confidentiality.

196. If the request is for more documents or additional information, then it is recommended that the agency be required to use its powers to compel the Firm to comply. This approach is not intended to be uncooperative or obstructive. However, insisting on compulsion will protect the Firm against accusations of breach of confidentiality. When the Firm is compelled in this way, client or other third-party consent is not required, and should not be sought because of the risk of tipping off.
197. Before responding to an order to produce information, Firms should make sure that they understand:

    a. the authority under which the request is being made;
    b. the extent of the information requested;
    c. the timetable and mechanism for providing the information; and
    d. what parts of the information should be excluded (i.e. because they are subject to legal privilege)

198. If in any doubt seek legal advice and always keep records of how the issues were judged.

Reporting to other bodies

199. Firms should have regard to their other obligations, such as their reporting responsibilities under the International Auditing Standards, statutory regulatory returns, or the reporting of misconduct by fellow members of a professional body and the Cayman Islands Ombudsman[6]. In all these cases the risk of tipping off must be considered and the offence avoided. Accountants may wish to contact CIIPA for advice, or else seek legal advice.
200. A tipping off offence is not committed under POCL if the person did not know or suspect that they were likely to prejudice any subsequent investigation. Situations in which this defence may apply include:

    a. reporting to one's own professional body if it is an anti-money laundering supervisor;

    b. reporting a matter of material significance to the Cayman Islands Monetary Authority.

[6] According to the Whistleblower Protection Law

F. RECORD KEEPING

201. Records relating to CDD, including non-engagement documents relating to client relationships, any transactions and correspondence must be kept for at least **five years from the end of the client relationship**. A disengagement letter is documentary evidence that a business relationship has terminated, but other forms of communication such as emails may suffice.
202. All records related to a one-off transaction must be retained for five years after the **date of the transaction**.
203. The AML Regulations do not specify the form in which records should be kept, but they must be readily retrievable.
204. No retention period is officially specified for records relating to:
    a. internal reports;
    b. the MLRO's consideration of internal reports;
    c. any subsequent reporting decisions;
    d. issues connected to consent, production of documents and similar matters;
    e. suspicious activity reports and consent requests sent to the FRA, or its responses.

but since these records can form the basis of a defence against accusations of money laundering and related offences, Firms should determine and apply a suitable retention period.

205. Records related to internal and external reports of suspicious activity are not part of the working papers relating to client assignments. They should be stored separately and securely as a safeguard against tipping off and inadvertent disclosure to someone making routine use of client working papers.
206. Firms must demonstrate their compliance with AML Regulations that place a legal obligation on them to make sure that certain of their employees are, (a) aware of the law relating to money laundering and terrorist financing, and (b) trained regularly in how to recognise and deal with transactions and other events which may be related to money laundering or terrorist financing. Records should show the training that was given, the dates on which it was given, which individuals received the training and the results from any assessments.
207. Firms must balance the requirements of POCL and AML Regulations with the requirements of the **Data Protection Law ("DPL")**. The DPL requires that personal information be subject to appropriate security measures and retained for no longer than necessary for the purpose for which it was originally acquired.

208. Section 8 of the DPL grants a right for individuals to access their own personal data, as well as certain information about the data (listed in section 8(1) and (2)). CDD is personal data, and therefore the access right applies to it, unless an exemption applies that nullifies that right. It is possible that the exemption in section 19 may apply to such processing, since the purpose of the processing is the detection of crime (whether or not the data subject actually broke the law). However, a firm that holds the data and wishes to apply the exemption would have to be able to demonstrate that providing the data to the individual "would be likely to prejudice" the detection of crime (i.e. with a relatively high level of certainty). Whether or not it does, will depend on the circumstances. Similarly, personal data that relates to knowledge or suspicion of money laundering (i.e. data that has been processed to help prevent or detect crime) need not be disclosed under a subject access request if to do so could constitute tipping off.

209. Data exempt from one subject access request may no longer be exempt at the time of a subsequent request (perhaps because the original suspicion has by then been proved false). When a Firm receives a data subject access request covering personal data in its possession, it should always consider whether the exception applies to that specific request regardless of any history of previous requests relating to the same data. These deliberations will usually involve the MLRO and the data protection controller. It is recommended that the rationale behind any decision to grant or refuse access is documented.

210. Once the retention periods have expired, the Firm should delete any personal data unless -

    a. The Firm is required to retain under statutory obligation,
    b. the Firm is required to retain it for legal proceedings, or
    c. the data subject has consented to the retention.

G. TRAINING AND AWARENESS

211. The AML Regulations require that all employees are:
    a. made aware of money laundering, terrorist and proliferation financing and targeted financial sanctions laws;
    b. made aware of the Firm's policies and procedures; and
    c. trained regularly to recognise and deal with transactions which may be related to money laundering, terrorist or proliferation financing and targeted financial sanctions, as well as to identify and report anything that gives grounds for suspicion.
212. A formal training plan can help make sure that the right staff receive the right training to enable them to comply with their obligations but if in doubt basic training should be provided to all staff.

What should be included in the training?

213. Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them. The key is to ensure engagement by staff as to the importance of the training.
214. The programme itself should include:
    a. an explanation of the law within the context of the business's own commercial activities;
    b. the Firm's policies and procedures; and
    c. how to deal with transactions that might be related to ML/TF/PF/TFS (including how to use internal reporting controls), the business's expectations of confidentiality, and how to avoid tipping off.

215. Where applicable, training programmes should be tailored to each business area and cover the firm's procedures so that staff members understand the ML/TF/PF/TFS risks posed by the specific services they provide and types of client they deal with. Furthermore, Firms should aim to create an culture in which staff are always alert to the ML/TF/PF/TFS risks and habitually adopt a risk-based approach to client due diligence.
216. A system of tests, or some other way of confirming the effectiveness of the training, should be conducted, either separately or as part of the employees performance appraisal.

When should training be completed?

217. Firms should ensure that new staff are trained within one month of appointment. Where this is not possible for unavoidable reasons then controls should be employed to reduce any risks arising from the lack of training.
218. The frequency of training events can be influenced by changes in legislation, regulation, professional standards, case law and judicial findings (both domestic and international), as well as by changes in the business's risk profile and procedures.
219. Otherwise it may not be necessary to repeat a complete training programme annually, but it may be appropriate to provide employees with concise updates to help refresh and expand their knowledge and to remind them of the importance of effective AML CFT controls. There are always matters and topics arising that related to AML and CFT to provide training on.
220. In addition to training, Firms are encouraged to run periodic AML awareness campaigns to keep staff alert to individual and firm-wide responsibilities.

H. AML/CFT AUDIT

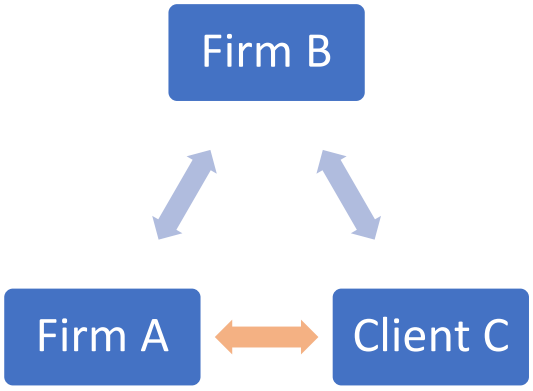
221. Firms carrying on relevant financial business must introduce a system of regular independent audits, so that the adequacy and effectiveness of systems can be better understood and any weaknesses systematically identified, in order that recommendations for improvement can be made and compliance monitored. When changes are made to controls these should be properly communicated to staff and supported by appropriate training where necessary.
222. This may entail:
    a. Internal audit
    b. Internal/external compliance review, and/or
    c. Adaption of cold reviews

223. However, the key is that the audit or review is an assessment that feeds into the Firm's risk-based approach to its controls. It is closely related to the risk assessment.

224. A sole practitioner who has no employees need not establish an AML/CFT audit to be performed by another person, because it would not be appropriate to the size and nature of the business. It does not make sense to review files as the sole practitioner has done all the work him or herself. More importantly, the sole practitioner must regularly review its ML and TF PF risk and this requires them to step back and review the business objectively which can be as effective as an AML/CFT/CFP audit.
225. If, however any staff are employed certainly in a professional and possibly in administrative capacity that is client facing, then appropriate internal audits/reviews are required.

I. OUTSOURCING, SUBCONTRACTING AND SECONDMENTS

226. The Firm must consider whether outsourcing/subcontracting its business functions increases the risk that it will be involved in, or used for, MLTF, in which case appropriate controls to address that risk should be put in place.
227. Where a Firm A, is engaged by another professional services Firm B, to help with work for one of its clients or some other underling party, C, then A should consider whether its client is B, or C. For example, where there is no business relationship formed, nor is there an engagement letter between the two,



it may be that CDD on C is not required but should instead be completed for the professional services firm itself, B.

228. On the other hand, where there is significant contact with the underlying party, or where a business relationship with it is believed to have been established, then C may also be deemed a client and CDD may be required for both C and B. In this situation A may wish to take into account information provided by B and the relationship it has with C when determining what CDD is required under its risk-based approach. It should be noted that the same considerations are relevant in networked arrangements, where work is referred between member firms.

229. The Firm is responsible for conducting CDD on its clients to Cayman Islands standards, including maintaining the appropriate records even if execution of all or part of the client work is outsourced or sub-contracted out. Some aspects of CDD such as collecting documentary evidence can also be delegated to an outsourcer or sub-contractor, but the Firm or individual remains responsible for compliance with Cayman Islands legislation.

230. The Firm remains responsible for reporting any knowledge or suspicion of MLTF that comes to it in the course of its own business, but not for reporting knowledge or suspicion that comes to the attention of the outsourcer or subcontractor, if that is not passed on to the Firm. When a sub-contractor is integrated into a Cayman Islands business its staff should be trained in the Firm's AML CFT policies and procedures.

Outsourcing Compliance

231. A Firm may arrange for another organisation to perform some of its AML-related functions. Outsourcing to others to complete all or part of CDD[7] or to delegate the compliance function in whole or part is only permitted if the other party is a member of the regulated sector in the Cayman Islands, or be subject, in an equivalent country, to an equivalent regulatory regulator and equivalent regulatory supervision requirements. Equivalent countries are those assessed and reported as such by the Anti Money Laundering Steering Group ("AMLSG") https://www.cima.ky/list-of-equivalent-jurisdictions. (see Regulation 22, 24/25).

232. Further, the Firm should

    a. ensure that the other party's record keeping procedures are good enough to demonstrate compliance with the AML obligations, or else it must obtain and maintain copies of the records for itself.

    b. consider how it would obtain its records from the other party should they be needed, as well as what would happen to them if the other party ceased trading.

[7] Regulations 24 and 25

c. enter into a written agreement to ensure that the other party will provide the CDD immediately on request.

233. An arrangement of this kind can be useful and efficient when the two parties are able to build a relationship of trust, but it should not be entered into lightly. Liability for inadequate CDD remains with the Firm, so Firms placing reliance on another should satisfy themselves with the level of CDD being undertaken.

Firms granting reliance

234. A Firm should consider whether it wishes to be relied upon to perform CDD for another organisation. Before granting consent, a Firm must ensure that their client (and any other third party whose information would be disclosed) is aware that the disclosure may be made to the other party and has no objection to the disclosure and other aspects of the Data Protection Law are complied with. Further the Firm should make sure that:

a. it has adequate systems for keeping proper CDD records;
b. it can make available immediately on request:
   - any information about the client/BenO gathered during CDD; and/or
   - copies of any client/BenO identity/verification data or documentation obtained during CDD,
c. it can keep those CDD records securely for five years.

Secondments

235. A secondee is an individual employed by one organisation (the seconder) but acting as an employee of another (the receiver). The formal terms of all secondments should address how the obligations imposed by the AML regime will be applied.

236. When secondees are instructed and supervised only by the receiver, they must be subject to its AML/CFT policies and procedures and the receiver should ensure that the secondee receives appropriate training. Where the seconder also provides defined services, the training may relate solely to the receiver's procedures, which may differ from the those of the receiver.

Reporting requirements for subcontractors and secondees

237. Where all or part of a piece of work is contracted-out there is no legal requirement for the subcontractor to report suspicious activity to the referring business's MLRO. However, where the subcontractor does notify the referring business of information which gives rise to a money laundering suspicion, the referring business must consider its own reporting obligations.

238. Similarly, where a secondee brings information, in the course of business, into the seconding business, the seconding business must consider its own reporting obligations.
239. The position of an individual working temporarily outside the Cayman Islands on secondments or working permanently outside the Cayman Islands but still within a Firm is more difficult. For example, the duty to report may be influenced by the terms of the secondment or arrangement. Firms or individuals may wish to take legal advice in relation to the need for their employees to comply with the Cayman Islands' reporting obligations as well as any local legal requirements.
240. Issues to consider include:
    a. If the work outside the Cayman Islands is part of a Cayman Islands regulated activity then in some circumstances it will be reportable.
    b. If an individual works permanently outside the Cayman Islands for a Cayman Islands firm, it may be appropriate to consider whether they are working at a separate firm or at a branch office of a Cayman Islands firm.
241. An individual should be particularly cautious about any decision not to make a report on their return to the Cayman Islands if the information relates to work that they are undertaking in the Cayman Islands.

Schedule 6 Proceeds of Crime Law

Activities falling within the Definition of "Relevant Financial Business"

Any activity related but not limited to -

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.
3. Financial leasing.
4. Money or value transfer services.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in –

    (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);

    (b) foreign exchange;

    (c) exchange, interest rate and index instruments;

    (d) transferable securities; or

    (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.

9. Advice to undertakings on capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings.
10. Money broking.
11. Individual and collective portfolio management and advice.
12. Safekeeping and administration of cash or liquid securities on behalf of other persons.
13. Safe custody services.
14. Financial, estate agency, legal and accounting services provided in the course of business relating to -

    (a) the sale, purchase or mortgage of land or interests in land on behalf of clients or customers;

    (b) management of client money, securities or other assets;

    (c) management of bank, savings or securities accounts; and

    (d) the creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
15. The services of listing agents and broker members of the Cayman Islands Stock Exchange as defined in the CSX Listing Rules and the Cayman Island Stock Exchange Membership Rules respectively.
16. The conduct of securities investment business.
17. Dealing in precious metals or precious stones, when engaging in a cash transaction of ten thousand dollars or more.
18. The provision of registered office services to a private trust company by a company that holds a Trust licence under section 6(5)(c) of the Banks and Trust Companies Law (2018 Revision).
19. Otherwise investing, administering or managing funds or money on behalf of other persons.
20. Underwriting and placement of life insurance and other investment related insurance.