



Legal Services
Supervisory
Authority

AML/CFT/CPF Guidance Notes

September 2026

TABLE OF ACRONYMS AND ABBREVIATIONS

TERM	MEANING
AIM	Alternative Investment Market
AML/CFT/CPF	Anti-Money Laundering/Counter the Financing of Terrorism/Counter Proliferation Financing
AMLCO	Anti-Money Laundering Compliance Officer
AMLRs	Anti-Money Laundering Regulations (2025 Revision)
AMLSG	Anti-Money Laundering Steering Group
BRA	Business Risk Assessment
CA	Competent Authority
CDD	Client Due Diligence
CFATF	Caribbean Financial Action Task Force
CIMA	Cayman Islands Monetary Authority
DAML	Defence Against Money Laundering
DMLRO	Deputy Money Laundering Reporting Officer
DNFBP	Designated Non-Financial Business or Profession
DPA	Data Protection Act (2021 Revision)
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FRA	Financial Reporting Authority
FSP	Financial Service Provider
HNWI/UHNWI	High Net Worth Individuals/Ultra-High Net Worth Individuals
IBA	International Bar Association
LLP	Limited Liability Partnership
LPP	Legal Professional Privilege
LSSA	Legal Services Supervisory Authority
MLRO	Money Laundering Reporting Officer
ML/TF/PF	Money Laundering/Terrorist Financing/Proliferation Financing
NPO	Non-profit Organisation
NRA	National Risk Assessment
PEP	Politically Exposed Person
PFPA	Proliferation Financing (Prohibition) Act (2017 Revision)
POCA	Proceeds of Crime Act (2025 Revision)
RBA	Risk-Based Approach
RFB	Relevant Financial Business
SA	Supervisory Authority
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SoW/SoF	Source of Wealth/Source of Funds
SRB	Self-Regulatory Body
TFS	Targeted Financial Sanctions
TA	Terrorism Act (2018 Revision)
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolutions

GLOSSARY

TERM	DEFINITION
Applicant for Business	A person seeking to form a business relationship or carry out a one off transaction with a person who is carrying out relevant financial business in the Islands.
Beneficial Owners	A beneficial owner is the natural person who ultimately owns or controls the client, or on whose behalf a transaction or activity is being conducted.
Business Relationship	Any arrangement between two or more persons where: (i) 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 (ii) 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.
Criminal Conduct	Conduct which constitutes an offence in any part of the Cayman Islands, or would constitute an offence in any part of the Cayman Islands if it occurred there. See Section 144(2) of the POCA.
Criminal Property	Property which constitutes, or represents, a person's benefit from criminal conduct (in whole or part and whether directly or indirectly), where the alleged offender knows or suspects that it is such and includes terrorist property. See Section 144(3) of the POCA and the definition of property.
Delegation	Performance of functions on behalf of the Supervised Firm and in accordance with the Supervised Firm's procedures.
Disclosure/Suspicious Activity Report	A report made to the FRA in accordance with Sections 136 and 137 of the POCA.
Dollar or \$	Cayman Islands dollars.
Financial Action Task Force	The FATF is an independent inter-governmental body established in 1989 that develops and promotes policies to protect the global financial system against ML/TF/PF.
Firms of Attorneys at Law	(i) a body corporate, association, partnership or limited liability partnership of attorneys who are admitted to practice law in the Islands; or (ii) an attorney admitted to practice law in the Islands who is in independent practice as a sole proprietor or who provides legal services to an employer other than the Government.
Inter Vivos Trust	A trust which takes effect while a person is alive. Also referred to as a Living Trust.
Legal Professional Privilege	LPP is a fundamental right established in the common law which requires legal professionals to maintain confidentiality in respect of communications and material evidencing such communication as it relates to legal advice and litigation.

GLOSSARY (cont.)

Money Laundering	The process by which the direct or indirect benefit of crime is channelled through financial or other systems to conceal the true origin and ownership of the proceeds of criminal activities.
Nominated Officer/Money Laundering Reporting Officer	A person nominated within the Practice to make disclosures to the FRA under the POCA.
One-Off Transaction	A transaction (carried out other than in the course of an established business relationship formed by a person conducting relevant financial business ("RFB")) amounting to CI\$10,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.
Outsourcing	A Supervised Firm's use of another entity (either an affiliated entity within a group or an entity that is external to the corporate group) to perform functions or activities on a continuing basis that would normally be undertaken by the Supervised Firm, now or in the future.
Overseas Criminal Conduct	Conduct which occurs in another jurisdiction that would constitute a criminal offence if it occurred in the Cayman Islands.
Politically Exposed Person	Politically Exposed Person, as defined in Regulation 2 of the AMLRs.
Practice	An independent legal practitioner's business, whether that business is a law firm, sole practitioner, recognised body or other entity carrying on business consisting of the provision of professional services such as are provided by individuals practising as attorneys at law.
Privileged Circumstances	Communications that are protected from disclosure and are exempt from certain provisions of the POCA. In many cases, such communication may also be protected by LPP.
Proliferation Financing	The act of providing funds, 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 or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Property	Includes money and all other property, real or personal, including things in action and other intangible or incorporeal property, and when used in relation to terrorism means, in addition, property likely to be used for the purposes of terrorism, proceeds from the commission of acts of terrorism or which has been used or is reasonably suspected to have been used, directly or indirectly, in the commission of an act of terrorism. See Section 2 of the POCA.

GLOSSARY (cont.)

Relevant Financial Business	As defined in Schedule 6 of the POCA; see section 1.3.2.
Reliance	Dependence on a third party by the Supervised Firm to perform CDD or to introduce business on its behalf
Supervised Sector	Activities, professions, and entities supervised for the purposes of AML/CFT/CPF obligations (See Chapter 1).
Regulations	Anti-Money Laundering Regulations (2025 Revision), as amended.
Supervised Firms	Firm of attorneys at law, including sole practitioners, carrying on relevant financial business within the legal sector of the Cayman Islands that are subject to supervision by the LSSA for compliance with the Anti-Money Laundering Regulations (2025 Revision).
Tax Adviser	A Practice which by way of business provides advice about the tax affairs of another person.
Terrorist Financing	The provision or collection of funds or other assets by any means, directly or indirectly, with the intention or knowledge that it be used to carry out terrorist acts or by a terrorist individual or entity.
Terrorist Property	Property that is the proceeds of, or used in, or intended or allocated for use in, the financing of acts of terrorism, terrorists or terrorist organisations.

CONTENTS

TABLE OF ACRONYMS AND ABBREVIATIONS	2
GLOSSARY	3
CHAPTER 1 – INTRODUCTION	9
1.1 Who this Guidance Applies To	9
1.2 Importance of AML/CFT/CPF Compliance	9
1.3 International Standards and Domestic Legal Framework	9
1.4 Supervisory and Enforcement Approach	12
1.5 Civil Liability Considerations	12
CHAPTER 2 – MONEY LAUNDERING	13
2.1 Introduction	13
2.2 POCA	14
2.3 Criminal Conduct and Criminal Property	14
2.4 Principal ML Offences	14
2.5 Defences to Principal ML Offences	15
2.6 Failure to Disclose	15
2.7 Tipping Off	16
2.8 ML Red Flags Highlighting Suspicious Activities or Transactions for Legal Professionals	16
CHAPTER 3 – TERRORIST FINANCING, PROLIFERATION FINANCING, & TARGETED FINANCIAL SANCTIONS	18
3.1 Introduction	18
3.2 What is Terrorist Financing?	18
3.3 Reporting Obligations	20
3.4 TF Vulnerabilities	21
3.5 Countering Proliferation Financing	23
3.6 Targeted Financial Sanctions related to Terrorism and Terrorist Financing and Proliferation Financing	23
CHAPTER 4 – SYSTEMS, POLICIES, PROCEDURES, AND CONTROLS	28
4.1 Introduction	28
4.2 Regulatory Obligations	28
4.3 Policies and Procedures	29
4.4 Senior Management Responsibility and Oversight	29
4.5 Compliance Function and AMLCO	29
4.6 MLRO and DMLRO	30
4.7 Sole Practitioners	30
4.8 Outsourcing and Reliance on Third Parties	31

4.9	Risk-Based Approach	31
4.10	Group-Wide Application	31
CHAPTER 5 – RISK-BASED APPROACH		33
5.1	Overview of the Risk-Based Approach	33
5.2	Business Risk Assessments	33
5.3	Application of Risk Assessments	39
5.4	Client Risk Assessments	40
5.5	Matter-Level Risk Assessments	41
5.6	Risk Weightings	42
5.7	Documenting Risk Assessments	42
5.8	Risk Mitigation	43
5.9	Monitoring of Controls	43
CHAPTER 6 – CLIENT DUE DILIGENCE		44
6.1	Purpose and Scope of Client Due Diligence	44
6.2	CDD Framework	44
6.3	When CDD is Required	45
6.4	Components of CDD	48
6.5	Timing and Completion of CDD	50
6.6	Methods of Identification and Verification	52
6.7	Source of Funds and Source of Wealth	59
6.8	Enhanced Due Diligence (EDD)	61
6.9	Politically Exposed Persons (PEPs)	63
6.10	Simplified Due Diligence (SDD)	64
6.11	Reliance on Third Parties	66
CHAPTER 7 – ONGOING MONITORING		68
7.1	Statutory Obligations and Scope	68
7.2	Scrutiny of Transactions	68
7.3	Refreshing and Reapplying CDD Measures	69
7.4	Evidence of Monitoring	70
CHAPTER 8 – RECORD KEEPING PROCEDURES		71
8.1	Obligations Under the AMLRs	71
8.2	Scope of Records to Be Retained	72
8.3	Group Records	72
8.4	Registers of Enquiries and Disclosures	73
8.5	Reliance and Delegation	73
8.6	Data Protection and Confidentiality	73

CHAPTER 9 – TRAINING	74
9.1 Importance of Training	74
9.2 Regulatory Requirement	74
9.3 Training Programme	74
9.4 Training for Sole Practitioners and Small Firms	76
9.5 Specific training for AMLCOs, MLROs and DMLROs	76
9.6 Training Records	77
CHAPTER 10 – SUSPICIOUS ACTIVITY REPORTING	78
10.1 Introduction	78
10.2 Application	78
10.3 Internal Reporting Procedures	79
10.4 Role of the MLRO	79
10.5 Suspicious Activity Reports	80
10.6 Defence Against Money Laundering / Consent Requests	81
10.7 Tipping Off and Prejudicing an Investigation	81
CHAPTER 11 – OTHER INTERNAL CONTROLS	82
11.1 Obligations under the AMLRs	82
11.2 Independent Audit Function	82
11.3 Employee Screening	84
11.4 Outsourcing and Third-Party Arrangements	84
CHAPTER 12 – LEGAL PROFESSIONAL PRIVILEGE	87
12.1 Introduction	87
12.2 Duty of Confidentiality	87
12.3 LPP	87
12.4 Privileged Circumstances	90
12.5 Differences between privileged circumstances and LPP	91
12.6 When do you Disclose?	92

CHAPTER 1 – INTRODUCTION

This Guidance is issued by the LSSA, in accordance with regulation 55D(1)(c) of the AMLRs, in its capacity as a Supervisory Authority, as established by the Cayman Islands Legal Services Council (LSC). This Guidance aims to provide an overview of the obligations of legal professionals under the AML/CFT/CPF regime.

This Guidance is provided to assist legal professionals in understanding and implementing their obligations pursuant to the AML/CFT/CPF framework and does not constitute legal advice.

1.1 Who this Guidance Applies To

This Guidance is applicable to all legal professionals and other staff employed by Supervised Firms, who play a role in the implementation of and compliance with the Cayman Islands AML/CFT/CPF regime. As this Guidance applies across the legal sector, the terms 'practice', 'firms of attorneys at law' or 'firms' are used to refer to a legal professional's business, whether that business is a law firm, or is conducted by a sole practitioner. For attorneys at law practising within a law firm, the term 'practice' refers to the firm or business as a whole and not a practice group within a firm.

While many obligations discussed in this Guidance arise where a legal professional conducts RFB, certain obligations under the Cayman Islands AML/CFT/CPF framework apply more broadly across the legal profession as a whole. In particular, legal professionals should be aware of their responsibilities relating to the reporting of suspicious activities and the implementation of TFS, which may arise regardless of whether or not they are conducting RFB.

1.2 Importance of AML/CFT/CPF Compliance

ML/TF/PF pose serious and longstanding threats to society. They can destabilise economies, endanger lives, fuel other criminal activity and produce significant cross-border effects. Criminals have used money laundering techniques to disguise the origins of illicit funds for decades, and may seek to use legal professionals to do so. It is therefore essential that legal professionals understand their AML/CFT/CPF obligations, uphold the ethical standards applicable to them, and avoid the risk of unintentionally assisting criminal activity.

1.3 International Standards and Domestic Legal Framework

1.3.1 Financial Action Task Force

The FATF is the global standard-setting body responsible for developing policies to combat ML/TF/PF. The FATF Recommendations are recognised as the international AML/CFT/CPF standards and ensure a co-ordinated global response to protect financial systems and the broader economy from misuse by criminals and terrorists.

The FATF monitors countries to ensure they implement the FATF Standards fully and effectively. In total, more than 200 jurisdictions have committed to implementing the FATF's Standards, which consist of 40 Recommendations and 11 Immediate Outcomes designed to ensure effective measures to prevent and detect ML/TF/PF.

The Cayman Islands is assessed against the FATF standards through the CFATF, one of nine (9) FATF-Style Regional Bodies, of which the Cayman Islands is a member country.

Countries, including the Cayman Islands, periodically undergo Mutual Evaluations (ME), which are peer reviews assessing both the technical implementation and effectiveness of AML/CFT/CPF measures. MEs provide an in-depth description and analysis of a country's AML/CFT/CPF system, as well as focused recommendations to further strengthen it. Stemming from the ME process, the FATF identifies jurisdictions with weak measures to combat ML/TF/PF in two FATF public documents issued three times a year. Placement on either of these lists (commonly referred to as the "Black List" or "Grey List") may have significant consequences for a country's economy and financial system.

The Cayman Islands' AML/CFT/CPF legislative framework is designed to align with these international standards.

1.3.2 Proceeds of Crime Act (2025 Revision)

Scope

The POCA establishes a number of ML offences including:

- the principal ML offences;
- the offences of failing to report suspected ML; and
- the offence of tipping off.

Further discussion of ML offences is provided in Chapter 2.

Application

The POCA applies to all persons, albeit certain offences only apply to nominated officers (see Section 137 of the POCA).

Schedule 6 of the POCA establishes the activities falling within the definition of RFB. In the legal sector, RFB includes legal services in the course of business relating to:

- the sale, purchase or mortgage of land or interests in land on behalf of clients;
- management of client money, securities or other assets;
- organisation of contributions for the creation, operation or management of companies;
- management of bank, savings or securities accounts;
- the creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

1.3.3 Terrorism Act (2018 Revision)

Scope

The TA establishes several offences including but not limited to terrorist offences, the financing of terrorism and the application of TFS. It also contains reporting obligations similar to those found under the POCA, particularly under Sections 23 and 25 (and Schedule 1), which apply where a person

knows, suspects or has reasonable grounds to suspect that another person has committed an offence under the TA (i.e. has had dealings with terrorist property).

However, as the definition of "criminal property" under the POCA includes terrorist property and the definition of "money laundering" under the AMLRs includes terrorist offences, reports relative to terrorism or dealings with terrorist property may also be made under the POCA regime.

Further discussion of these provisions is provided in Chapter 3.

Application

Section 29A. provides that Schedule 4A of the TA has effect for the purpose of empowering the Governor to — (a) propose the listing of a person as being involved in terrorist activities; (b) designate a person as being involved in terrorist activities; and (c) propose the delisting of a person who no longer meets the criteria for a designation as being involved in terrorist activities.

Section 23 of the TA imposes an obligation upon a person who believes or suspects that another person has committed an offence under Sections 19 to 22 of the TA (terrorist financing). Pursuant to Section 25 and Schedule 1 of the TA, similar obligations apply to persons in the regulated and public sectors. The principle of LPP applies under Schedule 1.

Where such knowledge or suspicion arises, a disclosure must be made to the FRA or to a Constable as soon as reasonably practicable. Such disclosure will not be treated as a breach of any statutory or civil duty of confidentiality. Failure to make a disclosure constitutes an offence.

Further details on the obligations of independent legal professionals under the TA are provided in Chapters 3 and 12.

1.3.4 Proliferation Financing (Prohibition) Act (2017 Revision)

Scope

The proliferation of weapons of mass destruction poses a significant threat to international peace and security. Therefore, it is essential that countries establish frameworks to deter, prevent and criminalise acts of proliferation financing. The PFPA is the foundation of such a framework in the Cayman Islands and provides for the implementation of TFS-PF. Further, the PFPA criminalises the financing of proliferation of weapons of mass destruction, as well as non-compliance with requirements imposed by directions issued under the law.

Application

Section 23A of the PFPA makes it an offence for any person to provide funds and economic resources to fund unauthorised proliferation activities, or to enter into or become concerned in an arrangement which that person knows, or suspects facilitates the acquisition, retention, use or control of funds and economic resources to fund such activities.

In addition to the criminalisation of PF, various provisions in the PFPA relate to the implementation of TFS. Section 3 of the PFPA empowers the FRA to give directions to persons specified under section 4 of the Act, in relation to a country, where measures are imposed by international organisations in

respect of that country. Pursuant to section 22 of the PFPA, a person who fails to comply with a requirement imposed by a direction under the Act commits an offence.

Further details on the obligations of legal professionals in respect of PF are provided in Chapter 3.

1.3.5 Anti-Money Laundering Regulations (2025 Revision)

Scope

The AMLRs form a central component of the Cayman Islands' AML/CFT/CPF framework.

The AMLRs were promulgated under the POCA and therefore have the force of law. The AMLRs have been in force for a number of years and are periodically revised to reflect developments in international standards and domestic policy. The 2025 Revision consolidates amendments made to the regulations and continues to establish the core AML/CFT/CPF obligations applicable to the supervised sector.

Application

The AMLRs apply primarily to persons carrying out RFB, as defined under Section 2 and Schedule 6 of the POCA.

1.4 Supervisory and Enforcement Approach

The LSSA is responsible for supervising firms of attorneys at law conducting RFB for compliance with the AMLRs. As a Supervisory Authority within the Cayman Islands' AML/CFT/CPF framework, the LSSA monitors compliance with regulatory requirements, promotes understanding of obligations within the legal sector, and works with other supervisory authorities, law enforcement agencies and other relevant authorities to address ML/TF/PF risks.

Breaches of AML/CFT/CPF obligations may result in supervisory, disciplinary or criminal consequences, depending on the nature and seriousness of the non-compliance. In addition to potential offences under applicable legislation, failures to comply with AML/CFT/CPF obligations may also constitute breaches of professional obligations applicable to firms of attorneys at law in the Cayman Islands.

Further information on the LSSA's enforcement powers is set out in the LSSA Enforcement Manual, which is available on the LSSA's website.

1.5 Civil Liability Considerations

In addition to potential regulatory or criminal consequences, legal professionals should be aware that involvement in transactions connected with criminal conduct may expose them to civil claims, including claims alleging that a professional adviser assisted in a breach of trust or fiduciary duty. Such claims may arise where a legal professional is alleged to have knowingly received or assisted in the misuse of client funds or assets.

Maintaining appropriate client due diligence, record keeping and internal controls can assist in demonstrating that reasonable steps were taken to identify and mitigate risks. Where legal professionals believe that they may be exposed to civil liability in connection with a matter, independent legal advice should be sought.

CHAPTER 2 – MONEY LAUNDERING

2.1 Introduction

ML is the process by which the direct or indirect benefit of crime is channelled through the financial system to conceal the true origin and ownership of the proceeds of criminal activities. Generally, to launder criminal proceeds, a money launderer places the proceeds in the financial system without arousing any suspicion, moves them through a series of complex transactions to obscure its original (criminal) source and finally, if successful, integrates it into the economy to make the funds appear to be derived legitimately.

The definition of ML in the POCA is sufficiently broad and includes not only committing the offences considered in this Guidance, but also inchoate offences such as attempt, conspiracy or incitement to commit such an offence, as well as aiding, abetting, counselling or procuring the commission of such an offence. Additionally, the principle of extraterritoriality applies whereby conduct occurring outside of the Cayman Islands which would constitute an offence (or an attempt, conspiracy or incitement to commit such an offence, as well as aiding, abetting, counselling or procuring the commission of such an offence) if committed in the Cayman Islands, will also constitute ML. (See *Section 144(10) of POCA*.)

ML has no single method. Criminals use a wide range of techniques of varying complexity to achieve their objectives. However, there are acknowledged stages of ML, namely, placement, layering and integration.

Placement

Placement refers to the introduction of proceeds, generated from criminal activity, into the financial system. This is typically the stage at which illicit funds are most apparent and therefore most susceptible to detection.

As financial institutions have strengthened their AML processes and procedures, criminals often seek alternative channels through which funds can be introduced into the financial system. Legal professionals may therefore be targeted due to the range of services they provide, including services that involve managing or handling client funds.

Layering

Once the proceeds of crime are placed in the financial system, layering involves separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. This stage often involves the use of entities, for example companies and trusts, and may take place across multiple jurisdictions. Legal professionals may become involved at this stage via the provision of services. Notably, detection at the layering stage can be particularly difficult.

Integration

Once the origin of the funds has been obscured by layering, the criminal is able to make the funds appear legitimate. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as legitimate funds. For example, this can be done by investing funds in legitimate businesses or other forms of investment, often using a legal professional to buy property, set up a trust, acquire a company, or even settle litigation, among other activities. This is the most difficult stage at which to detect ML.

2.2 POCA

Part 5 of the POCA establishes ML and other criminal conduct offences and criminalises ML pursuant to the international standards established in FATF R. 3 and on the basis of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (Vienna Convention) and United Nations Convention Against Transnational Organized Crime and the Protocols Thereto (Palermo Convention). The POCA also creates a disclosure regime and an offence for failing to make disclosures in relation to ML.

The POCA and the AMLRs apply to all legal professionals, although certain obligations apply specifically to those conducting RFB.

2.3 Criminal Conduct and Criminal Property

Pursuant to POCA, criminal conduct is conduct which constitutes an offence in any part of the Islands or would constitute an offence in any part of the Islands if it occurred there.

In relation to ML offences, property is criminal property if:

- (a) it constitutes a person's benefit from criminal conduct, or it represents such a benefit (in whole or part and whether directly or indirectly); and
- (b) the alleged offender knows or suspects that it constitutes or represents such a benefit.

The definition includes terrorist property.

2.4 Principal ML Offences

Section 133 – Concealing, disguising, converting, transferring or removing criminal property

A person commits an offence if he or she conceals, disguises, converts, or transfers criminal property, or removes criminal property from the Cayman Islands.

Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights with respect to it.

Section 134 - Arrangements

A person commits an offence if he or she enters into or becomes concerned in an arrangement which he or she knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

The term "arrangement" is not defined in the POCA. However, the arrangement must exist and have practical effects relating to the acquisition, retention, use or control of criminal property.

An agreement to enter into an arrangement will not always be an arrangement. The test is whether the arrangement does in fact, in the present and not the future, have the effect of facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person.

Section 135 - Acquisition, Use or Possession

A person commits an offence if he or she acquires, uses, or has possession of criminal property.

2.5 Defences to Principal ML Offences

A person may have a defence to a principal ML offence if:

- they make a disclosure to the FRA or a nominated officer (this does not apply to the person who committed or was a party to the act from which the property derives);
- they intended to make a disclosure to the FRA but had a reasonable excuse for not doing so;
- they are acting or carrying out a function they have relating to the enforcement of any provision of the POCA or of any other enactment relating to criminal conduct or benefit from criminal conduct;
- they are a professional legal adviser or other relevant professional adviser and the information or other matter came to them in privileged circumstances (see Chapter 12 for further guidance on legal professional privilege and privileged circumstances); or
- they know, or believe on reasonable grounds, that the criminal conduct occurred in a particular country or territory outside the Cayman Islands, and the relevant criminal conduct is:
 - not unlawful under the criminal law applying in that country or territory; and
 - is not of a description prescribed in an order made by the Attorney General of the Cayman Islands.

In relation to Section 135 of POCA, a defence may also apply where the property was acquired, used or came into possession for adequate consideration.

2.6 Failure to Disclose

Pursuant to section 136 of POCA, failure to make certain disclosures is an offence. A person is required to make reports of any information or other matter which comes to their attention and which, in their opinion, gives rise to:

- i. a knowledge or suspicion or reasonable grounds for knowing or suspecting that another person is engaged in ML;
- ii. a knowledge or suspicion or reasonable grounds for knowing or suspecting that the transaction or attempted transaction relates to ML.

A person commits an offence if:

- a) A person knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in criminal conduct;
- b) the information or other matter on which that person's knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to that person in the course of a business in the regulated sector or other trade, profession, business or employment;
- c) that person does not make the required disclosure to a nominated officer, or the Financial Reporting Authority, as soon as is practicable after the information or other matter mentioned in paragraph (b) comes to that person; and

- d) the required disclosure is a disclosure of —
- i. the identity of the person who may be involved in ML, if you know it;
 - ii. information or other matter in the form and manner prescribed by the AMLRs or the prior Act;
 - iii. the whereabouts of the property with respect to which the criminal conduct is committed, so far as that person knows it; and
 - iv. the information or other matter mentioned in paragraph (b), or prescribed under the AMLRs.

The abovementioned defences to the principal ML offences also apply in relation to failure to make a disclosure.

Where a practice has appointed a MLRO, disclosures should generally be made internally to that individual. The MLRO will consider the information and determine whether a disclosure should be made to the FRA.

Further guidance on internal reporting procedures and suspicious activity reporting is provided in Chapter 10.

2.7 Tipping Off

The offence of tipping off in relation to ML is contained in section 139 of the POCA. Similar tipping off offences exist in relation to terrorist property under the TA.

A person commits the offence of tipping off if he or she knows or suspects that an activity in relation to which a disclosure must be made under the POCA is about to take place, is taking place or has taken place (whether or not a disclosure has been or is likely to be made in relation thereto), and he or she makes a disclosure which is likely to prejudice any investigation which might be conducted following the disclosure which was required (whether or not the investigation is conducted).

2.8 ML Red Flags Highlighting Suspicious Activities or Transactions for Legal Professionals

Unusual Transactions

- Transactions that are unusual due to their size, nature, frequency, or manner of execution;
- Significant differences between the declared price of an asset and its apparent market value;
- Legal persons or arrangements, including NPOs, requesting services for purposes or transactions, that are inconsistent with their stated objectives or activities;
- Transactions which involve disproportional amounts of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.
- Securities transferred at prices that appear significantly above or below market value when compared to relevant indicators such as revenue, business activity, assets or financial performance.

Unusual Source of Funds

- Third party funding with no apparent connection or legitimate explanation;
- Funds received from or sent to foreign jurisdictions with no apparent connection to the client;
- Funds received from or sent to high-risk jurisdictions;
- Collateral for a transaction being located in a high-risk jurisdiction

Unusual Financial Behaviour

- Use of multiple or foreign bank accounts without good reason.
- Unusually short repayment period has been set without logical explanation;
- Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation;
- Assets purchased with cash and then subsequently used as collateral for a loan.
- Requests to change previously agreed procedures without logical explanation, especially when unusual payment instruments are proposed;
- Significant sums contributed in cash as collateral rather than being used directly for the transaction;

Unusual Corporate or Asset Activity

- Significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation.
- Injections of capital or assets in kind that is excessively high in comparison with the business, size or market value of the company performing, with no logical explanation.

CHAPTER 3 – TERRORIST FINANCING, PROLIFERATION FINANCING, & TARGETED FINANCIAL SANCTIONS

3.1 Introduction

TF is an ever-evolving threat, with terrorist actors continually adapting their methods of raising, moving, storing and using funds to exploit the international financial system and sustain terrorist activity.

As highlighted in the FATF Report on Comprehensive Update on TF Risks¹, various methods are employed by terrorist individuals and entities in the financing of terrorism, and may include the use of cash, hawala networks, money value transfer services, online payment services, formal financial services, digital platforms, and virtual assets. Terrorist actors may also seek to exploit legal entities and arrangements including companies, trusts and other structures, to move or obscure funds. The report also notes the increase in the mixed use of diverse financing methods and the integration of digital technologies with conventional techniques, adding new layers of complexity to TF activities.

Notably, TF differs from ML in that funds used to support terrorist activity may originate from both legitimate and illegitimate sources. The involvement of both legitimate and illegitimate funds, alongside the misuse of various actors, are often involved in the various stages of TF. In the circumstances, detection of TF can be particularly challenging. Legal professionals should therefore remain alert to circumstances where legal services could be misused to facilitate the raising, movement, storage or use of funds for terrorist purposes. Further, it is essential that legal professionals protect themselves from misuse by terrorist individuals and entities via the implementation of an RBA to actively counter the financing of terrorism.

3.2 What is Terrorist Financing?

TF is the provision or collection of funds or other assets by any means, directly or indirectly, with the intention or knowledge that it be used to carry out terrorist acts or by a terrorist individual or entity.

The primary goal of individuals or entities involved in TF is to conceal both the financing and the nature of the financed activity to achieve their end goal of committing or facilitating terrorist acts. TF activities commonly involve several stages, including the raising, moving, storing and use of funds or other assets.

- Raising: This stage involves collecting or generating funds and other assets from one or multiple sources. This may involve the collection of legitimate funds from donations, the use of charities and NPOs, funds from legitimate business operations, self-funding from salaries and can also span to the collection of funds from illegitimate means such as extortion, human trafficking and other criminal activities.
- Moving and Storing: After acquiring funds and other assets, terrorist individuals and entities usually move and store those funds in an effort to conceal them without their intentions and actions being detected. These stages usually involve the use of the wider financial system and include a range of

¹ FATF Report- Comprehensive Update on Terrorist Financing Risks, July 2025 <https://www.fatf-gafi.org/en/publications/Methodsand Trends/comprehensive-update-terrorist-financing-risks-2025.html>

methods which often involve cross border transactions. Some mechanisms used include the use of cash couriers, MVTs, financial institutions, VA and VASPs, hawala systems inter alia.

- Using: The final stage involves the use of funds and other assets to carry out terrorist acts, fund terrorist organisations, FTF travelling, purchase weapons and equipment, facilitate training, and support a range of other terrorist-related activities.

3.2.1 International Standard

FATF & UNSCRs

FATF Recommendation 5 establishes the international standard for the creation of TF offences. FATF Recommendation 5 and its Interpretive Note (INR.5) set out in detail the specific elements required to comply with the obligation to criminalise TF based on the International Convention for the Suppression of the Financing of Terrorism (1999) (the TF Convention) and relevant UNSCRs.

Recommendation 5 further provides that it should also be an offence to attempt, participate as an accomplice, organise or direct others and contribute to the commission of a TF offence.

The measures employed by jurisdictions to counter TF vary as countries have diverse legal, administrative and operational frameworks and different financial systems. The FATF Recommendations, therefore, set an international standard which countries should implement through measures adapted to their particular circumstances.²

In addition, the UNSC has established UNSCRs which set out mandates for compliance by member states to counter TF. UNSCR 1373(2001), 2253(2015), 2396(2017), 2462 (2019) are a few of the many UNSCRs which calls on member states to, amongst other things:

- take measures to prevent and suppress the financing of terrorism, terrorist organisations, and individual terrorists even in the absence of a link to a specific terrorist act, including from the proceeds of organised crime, inter alia;
- criminalise the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;
- freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;
- prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or

² 2012 FATF Recommendations

indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons; and

- recognise the need for member states to complement international cooperation by taking additional measures to prevent and suppress, in their territories through all lawful means, the financing and preparation of any acts of terrorism.

The FATF standards and UNSCRs form the foundation upon which many jurisdictions build their CFT frameworks, as members of both FATF/FSRB and the UN.

International Convention for the Suppression of the Financing of Terrorism (1999)

Article 2(1) of the TF Convention provides:

“Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part...”

Importantly, for an act to constitute an offence as set out above, it shall not be necessary that the funds were in fact used to carry out or attempt a terrorist act.

3.2.2 Domestic Framework

The Terrorism Act (2018 Revision) criminalises TF.

Pursuant to section 18, “terrorist property” means property that is the proceeds of, or used in, or intended or allocated for use in, the financing of acts of terrorism, terrorists or terrorist organisations.

The range of TF offences established under Part III (sections 19-22) of the TA includes:

- Soliciting terrorist property (which comprises all the key elements of the Art.2(1) of the TF Convention)
- Use and possession of terrorist property
- Arranging for property to be used for terrorist purposes
- Laundering of terrorist property

3.3 Reporting Obligations

Pursuant to the legislative framework of the Cayman Islands, firms of attorneys at law have certain reporting obligations in respect of TF which are primarily encompassed in the TA and the AMLRs.

3.3.1 The TA

Section 25 and Schedule 1: Schedule 1 of the TA sets out a list of conditions which, if satisfied, results in the commission of an offence. A person within the regulated sector, including legal professionals as DNFBPs, commits an offence if he:

- knows or suspects, or has reasonable grounds for knowing or suspecting, that another person has committed an offence under sections 19 to 22;
- the information or other matter on which his knowledge or suspicion is based or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector; and
- does not disclose the information or other matter to a constable or a nominated officer as soon as is practicable after it comes to him.

Exception: A person does not commit an offence on the basis of the foregoing if he is a professional legal adviser and the information or other matter came to him in privileged circumstances. For these purposes, information or other matter comes to a professional legal adviser in privileged circumstances if it is communicated or given to him:

- (i) by a client or by a representative of a client in connection with the giving by the adviser of legal advice to the client;
- (ii) by a person seeking legal advice or by a representative of a person seeking legal advice from the adviser; or
- (iii) by a person in connection with legal proceedings or contemplated legal proceedings.

This exception does not apply to information or other matters communicated with a view to furthering a criminal purpose.

Accordingly, legal professionals must disclose knowledge, suspicion or reasonable grounds for believing that another person has committed a TF offence, where such knowledge or suspicion arises in the course of business and does not fall within the scope of privileged circumstances or LPP.

3.3.2 The AMLRs

Pursuant to regulation 19 of the AMLRs, a person carrying out RFB is required to file a SAR where he:

- (a) forms a suspicion of ML, TF or PF; and
- (b) reasonably believes that satisfying ongoing CDD requirements under the AMLRs for a customer or CDD requirements of the AMLRs for an applicant for business will tip off a customer or an applicant for business,

In such circumstances, legal professionals should not complete the CDD requirements under the AMLRs and must instead file a SAR relative to the suspicion.

3.4 TF Vulnerabilities

*The FATF Report on Comprehensive Update on Terrorist Financing Risks 2025*³ entails information on the various methods used to raise, move and manage funds and other assets for TF purposes. One of the aforesaid categories included methods based on the abuse of legal entities. This method may often involve the procurement of legal services in respect of the formation and/or management of legal persons and legal arrangements.

The report detailed that corporate vehicles such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements can be vulnerable to TF exploitation, as their involvement in a wide

³ FATF Report on Comprehensive Update on Terrorist Financing Risks 2025 <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf>

range of commercial and entrepreneurial activities make them attractive tools for circumventing CFT measures and facilitating other illicit purposes.

Primarily, delegations reported the use of shell companies, the creation of enterprises in multiple jurisdictions and investment on multilayer schemes involving big and small business for TF purposes. Due to disruption activities employed by competent authorities, terrorist individuals and entities are shifting from traditional methods to more complex schemes to raise, move, store, and spend their funds.

Several delegations mentioned the use by terrorist companies of front and shell companies to move funds with increased opacity. Methods based on front and shell companies differ from the ones based on formal economic activities, as they don't rely on legal persons to generate revenue through an actual economic activity, but only use the administrative opportunities offered by the legal person: emitting invoices, opening bank accounts, and operating transfers. There can also be schemes where companies with licit activities are used as front for TF purpose. In those occasions, licit and illicit funds are mixed, making detection even harder.

Those methods pursue two primary aims:

1. moving funds internationally through the regulated financial system, or
2. to launder funds from illicit resources to ultimately invest them in formal businesses.

When establishing such schemes, terrorist organisations can exploit vulnerabilities offered by weak regulatory framework, as well as vulnerabilities emerging from varying regulatory standards from one jurisdiction to the other, as well as shortcomings in international cooperation, making it harder to detect fraudulent transactions operated between two legal persons located in different jurisdictions.

Relying on front and shell companies requires some legal and administrative knowhow, and many delegations which reported such cases indicated those schemes were rare and complex. As such, criminals may secure the services of attorneys at law in establishing those complex structures and schemes.

*The FATF Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*⁴ outlined the top four areas of vulnerabilities identified by legal professionals:

- Purchase and sale of real property;
- Formation, merger, acquisition of companies;
- Formation of trusts; and
- Providing company or trust services.

In addition, legal professionals in several jurisdictions identified probate, tax advice and work involving charities as areas that gave rise to circumstances requiring the filing of a SAR.

The Cayman Islands National Risk Assessment (NRA) provides additional analysis of TF risks relevant to the jurisdiction. Legal professionals should consider the findings of the NRA when assessing potential risks within their practice.

⁴ FATF Report on Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, June 2013 <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf.coredownload.pdf>

3.5 Countering Proliferation Financing

Proliferation of weapons of mass destruction is the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services, and expertise.

The proliferation of weapons of mass destruction poses a significant threat to international peace and security. This threat is internationally recognised by the United Nations in various UNSCRs, the FATF in its standards and by other international bodies and conventions.

PF refers to the act of providing funds or financial services which are used, in whole or in part, to enable proliferation of weapons of mass destruction. PF extends beyond the direct payment for goods and includes any financial service provided in support of any part of the procurement process, even if it is not directly connected to the physical movement of goods. Financing may include financial transfers, mortgages, credit lines, insurance services, middlemen services, trust and corporate services and company formation.

PF facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items poses risks to global security and stability and may ultimately result in loss of life.

International standards require jurisdictions and regulated entities to identify and mitigate PF risks. This includes recognising potential breaches, non-implementation or evasion of targeted financial sanctions related to PF, and taking appropriate mitigating measures commensurate with the level of risk identified.

The PFFA makes it an offence for any person to provide funds and economic resources to fund unauthorised proliferation activities, or to enter into or become concerned in an arrangement which that person knows or suspects facilitates the acquisition, retention, use or control of funds and economic resources to fund such activities.

A person acting in the course of a business in the financial sector may commit an offence, even where the relevant conduct takes place wholly or partly outside of the Cayman Islands.

3.6 Targeted Financial Sanctions related to Terrorism and Terrorist Financing and Proliferation Financing

TFS entails both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.⁵

FATF & UN Security Council Sanctions Regimes

FATF Recommendation 6 and Immediate Outcome 10 establish international standards for assessing the technical compliance and effectiveness of countries' TFS frameworks. These standards incorporate the mandates of various UNSCRs relating to the prevention and suppression of terrorism and TF. The primary aim of all UN sanctions, as set out in Chapter VII of the UN Charter, is to implement decisions by the UNSC for the maintenance of international peace and security.

⁵ FATF Glossary

Recommendation 6 requires countries to implement TFS-TF without delay (within a matter of hours and no more than twenty-four (24) hours from the designation) by freezing the funds and other assets of designated individuals and entities and ensuring that no funds, assets or financial or other services are made available to them. The implementation of TFS-TF relates to both:

- (1) the UNSC sanctions regimes on ISIL (Da'esh) & Al-Qaida (UNSCR 1267(1999) and the Taliban (UNSCR 1988(2011)); and
- (2) Domestic Sanctions Regimes (UNSCR 1373 (2001)).

Effective asset freezing regimes are critical to combating TF and, as a preventive tool, accomplish much more than freezing terrorist-related funds or other assets. Effective freezing regimes also combat terrorism by⁶:

- (a) Deterring non-designated persons or entities who might otherwise be willing to finance terrorist activity.
- (b) Exposing TF “money trails” that may generate leads to previously unknown terrorist cells and financiers.
- (c) Dismantling TF networks by encouraging designated persons or entities to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups.
- (d) Terminating terrorist cash flows by shutting down the pipelines used to move terrorist related funds or other assets.
- (e) Forcing terrorists to use more costly and higher-risk means of financing their activities, which makes them more susceptible to detection and disruption.
- (f) Fostering international co-operation and compliance with obligations under the Al-Qaida/Taliban sanctions regimes, and resolution 1373(2001).

FATF Recommendation 7 and Immediate Outcome 11 require the implementation of TFS related to proliferation of weapons of mass destruction. These measures complement UNSCRs with respect to PF, including:

- The global approach aimed at preventing non-state actors from participating in proliferation-related activities (UNSCR 1540 (2004) and its successor resolutions).
- The country-specific approach against the Democratic People’s Republic of Korea (DPRK) pursuant to UNSCR1718 (2006) and successor resolutions.
- The country-specific approach against Iran pursuant to UNSCRs 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1929 (2010).

Essentially, jurisdictions must ensure that proliferation-related assets are frozen and that appropriate national mechanisms exist to implement these measures effectively.

⁶ Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6), FATF, June 2023 <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-Fin-Sanctions-TF-R6.pdf.coredownload.pdf>

Cayman Islands TFS Sanctions Regime

In the Cayman Islands the sanctions regime framework is built on the following⁷:

- Sanctions and Anti-Money Laundering Act (SAMLA) 2018;
- The Counter-Terrorism (Sanctions) (Overseas Territories) Order 2020;
- The Terrorism Act (2018 Revision); and
- The Proliferation Financing (Prohibition) Act (2017 Revision).

Notably, the Cayman Islands imposes the Sanctions Regimes of the UN and UK but can also impose its own financial sanctions and restrictions.

The financial sanctions in force in the Cayman Islands are essentially the same as those imposed in the UK. The Foreign, Commonwealth & Development Office (FCDO) publishes the UK Sanctions List which is now the sole source for current UK sanctions designations, and provides details of those individuals and entities designated under sanctions regimes set up using the powers in SAMLA (including designations made under the UNSC Sanctions Regimes).

As a British Overseas Territory, the Cayman Islands is obligated to implement the sanctions agreed at the UN and in the UK, in order to ensure compliance with international obligations and policy commitments. Thus, by virtue of the Counter-Terrorism (Sanctions) (Overseas Territories) Order 2020, all designations made under UN and UK sanctions measures have immediate effect in the Cayman Islands. All new or amended Overseas Territories Orders in Council (OOC) are gazetted in the Cayman Islands.

The current OOCs that give effect to TFS-TF in the Cayman Islands are relative to:

- UNSCR 1267 (1999) and UNSCR 1988 (2011)
- Domestic Designations pursuant to UNSCR 1373 (2001)
- UNSCR1718 (2006) and successor resolutions in respect of DPRK.
- UNSCRs 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1929 (2010) in respect of Iran.

All natural and legal persons, including RFB and non-RFB firms of attorneys at law, are required to comply with and implement TFS in force in the Islands, without delay, as per the foregoing. Firms should also consider its exposure to interactions with designated persons or entities under sanction regimes in countries in which they operate or have a nexus.

The PFPA established provisions to prevent and prohibit the financing of activities related to the proliferation of weapons of mass destruction. Key provisions include:

- (1) Designation of Individuals and Entities: The law allows for the designation of individuals and entities involved in PF.
- (2) Implementation of TFS: The law provides mechanisms for freezing the funds and economic resources of designated individuals and entities, as well as imposing prohibitions in respect of them.

⁷ Financial Reporting Authority, Financial Sanctions Guidance, December 2021 https://fra.gov.ky/wpfd_file/financial-sanctions-guidance-2/

- (3) Reporting Obligations: Individuals and entities that possess or control funds or other assets related to designated individuals and entities must report any frozen assets or actions taken to comply with the law to the Financial Reporting Authority.
- (4) Penalties for Non-Compliance: provisions for penalties against individuals or entities that fail to comply with its requirements, ensuring that the measures are effective and dissuasive.

For a comprehensive overview of all the sanctions regimes applicable to the Cayman Islands, please refer to the FRA's website: <https://fra.gov.ky/sanctions-regimes/>.

Implementation of TFS by Legal Professionals

Legal professionals should establish appropriate policies and procedures, to comply with sanctions measures as part of their overall AML/CFT/CPF compliance programme.

Legal professionals should also ensure that all relevant members of staff are adequately trained on the implementation of TFS. Information on Financial Sanctions Notices, sanctions lists, general licences, guidance and other relevant information on TFS are available via the FRA's website.⁸ Legal professionals must check sanctions updates and register for FRA website alerts to ensure implementation without delay.

Prior to entering into a business relationship with a client or carrying out a one-off transaction, legal professionals should screen clients, as well as beneficial owners and other relevant individuals and entities to ensure that they are not designated. Additionally, ongoing screening should be undertaken in respect of existing business relationships.

Where there is a true match or suspicion, legal professionals are required to comply with the sanctions obligations including reporting pursuant to the POCA, AMLRs, TA and PFPA.

Legal professionals are required to report to the Governor (through the FRA) as soon as practicable if:

- a) they know or have a reasonable cause to suspect that a person
 - i. is a designated person;
 - ii. has committed an offence under the legislation.
- b) the information, or other matter on which the knowledge or cause for suspicion is based, came to them in the course of carrying on their business.

Legal professionals are expected to keep track of all the applicable sanctions regimes, and where the sanction lists are updated, or during ongoing monitoring activities, ensure that existing clients are not listed. Legal professionals should subscribe to the FRA website by visiting <https://fra.gov.ky/all-sanctions/> and include their contact details. They should email FRA staff if they encounter issues with subscribing.

In relation to freezing and reporting, legal professionals must:

- (i) upon there being an addition or amendment to relevant sanctions list, determine without delay, whether they maintain any accounts or hold any funds, other assets or economic resources of a designated individual or entity;

⁸ <https://fra.gov.ky/all-sanctions/>

- (ii) immediately freeze such accounts, and other funds, other assets or economic resources which are owned or controlled by the designated individual or entity;
- (iii) not deal with the funds or economic resources or make them available to, or for the benefit of, the designated person unless there is an exception in the legislation that can be relied on, or if in possession of a licence from the Governor of the Cayman Islands; and
- (iv) report any findings to the FRA at financialsanctions@gov.ky, together with the information or other matter on which the knowledge or suspicion is based, by completing and submitting a Compliance Reporting Form⁹ (CRF). Where the information relates to funds or economic resources, the nature and quantity should also be reported. Information received by the FRA may be disclosed to third parties in accordance with provisions set out in the Information and record-keeping section of the regulations and in compliance with applicable data protection laws.

There is also a requirement that all persons that hold or control funds, other assets or economic resources owned, held or controlled by a designated individual or entity are to provide an annual frozen assets report to the Governor with details of these assets in the form of a report to the FRA¹⁰. Additionally, legal professionals must maintain records of any potential matches to names on sanctions lists regardless of whether the match turns out to be a true match or a false positive.

If any individual or entity is officially delisted, the obligation to implement TFS (i.e. the asset freeze and prohibition) no longer exists. If any funds or other assets have been frozen, they must be unfrozen.

In relation to unfreezing and reporting, legal professionals must:

- (i) determine whether they have frozen assets of any individual or entity no longer on the sanctions list and verify that the individual or entity is no longer subject to TFS;
- (ii) remove the person or entity from their internal list of individual and entities subject to TFS;
- (iii) take the necessary action to unfreeze the funds or other assets, accounts etc. of the individual or entity and where necessary resume the business relationship; and
- (iv) advise the FRA of the actions taken as soon as practicable.

Failure to comply with financial sanctions legislation or to seek to circumvent any provisions is a criminal offence which may result in criminal prosecution.

Legal professionals should document and record all the actions taken to comply with the sanctions frameworks, and the rationale for each action.

⁹ <https://fra.gov.ky/wpfd/file/compliance-reporting-form-2/>

¹⁰ <https://fra.gov.ky/frozen-assets-reporting-6-november-2025/>

CHAPTER 4 – SYSTEMS, POLICIES, PROCEDURES, AND CONTROLS

4.1 Introduction

This Chapter sets out detailed guidance for Supervised Firms on the systems, policies, procedures and controls that must be established, implemented and maintained in accordance with Part 2 of the AMLRs. It is intended to assist Supervised Firms in meeting their statutory obligations to prevent, detect and report ML/TF/PF, and to comply with TFS.

The systems, policies, procedures and controls apply to all persons carrying out RFB as set out in the AMLRs. Firms of attorneys at law must first assess whether they are carrying out any of the RFB activities listed in Schedule 6 of the POCA. Where a firm determines that it is in scope of the AMLRs, by virtue of conducting RFB, it is a Supervised Firm for the purposes of this Guidance and must comply with the AMLR obligations as set out in this Chapter.

This Chapter should be read as the structural foundation of the Guidance Notes. It explains what governance frameworks, compliance arrangements and control environments must exist within a Supervised Firm. Detailed guidance on how those requirements are applied in practice is addressed in subsequent chapters.

The systems, policies, procedures and controls adopted by a Supervised Firm must be proportionate to the nature, scale and complexity of its business and commensurate with the ML/TF/PF risks to which it is exposed, applying an RBA.

4.2 Regulatory Obligations

Part 2 of the AMLRs require every person carrying out RFB to establish and maintain a risk focused compliance programme comprising appropriate systems, policies, procedures and controls, and to ensure that employees are adequately trained in their application. Responsibility for compliance rests always with the Supervised Firm, notwithstanding any delegation, outsourcing or reliance on third parties.

Supervised Firms must develop and maintain AML/CFT/CPF systems which include, at a minimum:

- a) CDD measures;
- b) Implementation of an RBA;
- c) Internal policies, procedures and controls to combat ML/TF/PF, including appropriate compliance management arrangements;
- d) Adequate systems to identify ML/TF/PF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;
- e) Procedures to ensure compliance with TFS obligations;
- f) Record keeping procedures;
- g) Internal reporting procedures;
- h) Screening procedures to ensure high standards when hiring employees;
- i) An appropriate employee training programme;
- j) An audit function to test the AML/CFT/CPF system; and
- k) Where applicable, group-wide AML/CFT/CPF programmes.

4.3 Policies and Procedures

Supervised Firms must ensure that their AML/CFT/CPF policies and procedures are designed and implemented in a manner that supports the effective application of the firm's risk-based approach.

Policies and procedures must be clearly documented, approved by senior management and communicated to all relevant employees. They must be readily accessible and implemented in practice to ensure consistent and effective application across the firm. Approval by senior management may not be applicable to sole practitioners given the nature of their structure.

Policies and procedures should translate the requirements of the AMLRs and this Guidance into clear and practical instructions. In particular, they should:

- support consistent decision-making, including where judgement is exercised under the RBA;
- clearly define roles, responsibilities and escalation pathways; and
- ensure that AML/CFT/CPF obligations are embedded into the firm's day-to-day operations.

Supervised Firms must ensure that policies and procedures remain up to date and reflect changes in legislation, regulatory guidance, the firm's risk profile and its business activities.

4.4 Senior Management Responsibility and Oversight

Senior management has ultimate responsibility for the effectiveness of the Supervised Firm's AML/CFT/CPF framework. Senior management must approve the AML/CFT/CPF BRA and related policies and procedures and ensure adequate resources are allocated to AML/CFT/CPF compliance. Senior management should also ensure that they receive regular reports on the effectiveness of systems and controls, material breaches, suspicious activity and remedial actions to assist in fulfilling their duties. Additionally, senior management should foster a culture of compliance and ethical conduct throughout the Supervised Firm.

4.5 Compliance Function and AMLCO

Supervised Firms must establish and maintain a clearly defined compliance function with responsibility for overseeing compliance with the AMLRs and the ongoing effectiveness of the firm's AML/CFT/CPF framework. The compliance function should be appropriately resourced, independent from fee-earning activities where practicable, and proportionate to the nature, scale and complexity of the Supervised Firm and its ML/TF/PF risk exposure.

In accordance with regulation 3 of the AMLRs, Supervised Firms must designate an individual at the managerial level as the AMLCO. The AMLCO forms a core component of the compliance function and must have sufficient seniority, authority, independence and access to information to enable the effective discharge of the role.

The compliance function, operating under the oversight of the AMLCO, is responsible for:

- overseeing the implementation of the firm's RBA and ensuring that risk assessments are effectively embedded into operational controls;
- monitoring ongoing compliance with the AMLRs, applicable guidance and internal AML/CFT/CPF policies and procedures;
- coordinating AML/CFT/CPF training and awareness programmes to ensure employees understand their obligations;

- overseeing the effectiveness of internal controls, including outsourcing arrangements, employee screening processes and audit or independent review activities; and
- acting as the primary point of contact with competent authorities and the supervisory authority on AML/CFT/CPF matters.

The AMLCO must be able to escalate material compliance issues, significant control weaknesses and systemic breaches directly to senior management without undue delay. Notwithstanding the roles and functions of the AMLCO, senior management remains ultimately accountable for the adequacy and effectiveness of the Supervised Firm's AML/CFT/CPF compliance arrangements.

The compliance function may be structured flexibly, particularly within smaller Supervised Firms. However, all compliance responsibilities must be clearly allocated, appropriately documented and understood across the firm to ensure effective implementation and accountability. Supervised Firms must notify the LSSA of the appointment of the AMLCO, and of any subsequent change to that appointment, within thirty (30) days of the occurrence.

4.6 MLRO and DMLRO

Every Supervised Firm must appoint an MLRO in accordance with regulation 33 of the AMLRs. The MLRO must be employed at a managerial level and a suitably qualified and experienced individual with sufficient autonomy, authority and access to information to assess internal disclosures and determine whether a report should be made to the FRA.

The AMLCO and MLRO roles may be combined, provided that all statutory duties of both roles can be effectively discharged. Supervised Firms must also appoint a Deputy MLRO to ensure continuity and resilience.

Detailed guidance on suspicious activity reporting and internal procedures is provided in Chapter 10.

4.7 Sole Practitioners

Where a Supervised Firm operates as a sole practitioner, the compliance function may be discharged by the sole practitioner, who may simultaneously act as a fee earner, the AMLCO and MLRO. In such circumstances, the Supervised Firm should ensure that appropriate safeguards are in place to mitigate conflicts of interest and to maintain the effectiveness and objectivity of the compliance function. This includes ensuring that AML/CFT/CPF obligations are applied consistently across all matters, that risk assessments and compliance decisions are properly documented, and that sufficient time and attention are dedicated to compliance responsibilities alongside fee-earning activities.

The LSSA recognises that satisfying the Deputy MLRO requirement may present practical difficulties for a sole practitioner or a practice with only one fee-earner. Such practices should consult the LSSA regarding appropriate arrangements to ensure compliance with the AMLRs and continuity of the reporting function.

Sole practitioners should give particular consideration to the use of proportionate independent controls, such as external compliance support, peer review arrangements or periodic independent reviews, where appropriate, to support the effective discharge of AML/CFT/CPF obligations.

4.8 Outsourcing and Reliance on Third Parties

A Supervised Firm may, as part of a proportionate risk-based approach, outsource or obtain external support for elements of its AML/CFT/CPF framework. Such arrangements may be appropriate, particularly for smaller firms, however this does not transfer responsibility for compliance with the AMLRs, which remains at all times with the Supervised Firm, its partners and senior management.

Supervised Firms should ensure that any outsourcing or third-party arrangement is subject to appropriate governance, oversight and control, and does not impair the firm's ability to comply with its AML/CFT/CPF obligations, including duties of confidentiality and legal professional privilege.

Before entering into an outsourcing arrangement, the Supervised Firm must assess the risks associated with the arrangement and ensure that appropriate safeguards are in place to manage those risks. Supervised Firms must also ensure that they retain sufficient access to information, records and systems to enable effective oversight and compliance with regulatory and law enforcement requests.

Further detailed guidance on outsourcing arrangements and related internal controls is provided in Chapter 11.

4.9 Risk-Based Approach

Supervised Firms must adopt and document an RBA in accordance with Part 3 of the AMLRs. The RBA must be used to inform the design, implementation and calibration of AML/CFT/CPF systems, policies and procedures.

While detailed guidance on conducting risk assessments is set out in Chapter 5, Supervised Firms must ensure that systems and controls reflect the assessed risks relating to:

- clients and beneficial owners;
- jurisdictions and geographic exposure;
- services, transactions and delivery channels; and
- new products, services, business practices or technologies.

Decisions taken under the RBA, including the application of simplified or enhanced measures, must be documented and capable of being justified to the LSSA upon request.

4.10 Group-Wide Application

Supervised Firms should consider the application of the AMLRs to their wider group, where applicable. Where a firm in the Cayman Islands operates branches, affiliates, representative offices or majority-owned or controlled subsidiaries in any other jurisdiction, it must establish and maintain group-wide AML/CFT/CPF compliance programmes and comply with the relevant requirements of the AMLRs.

In relation to branches and majority-owned subsidiaries, Supervised Firms should, before relying on group-wide AML/CFT/CPF programmes, conduct and document a gap analysis between the group-wide programmes and the local AML/CFT/CPF legislative and regulatory requirements. The purpose of the gap analysis is to ensure that group-wide programmes meet, at a minimum, the applicable Cayman Islands requirements.

Supervised Firms should also conduct and document a gap analysis whenever there are material changes to:

- local AML/CFT/CPF legislation or regulatory guidance; or
- the group-wide AML/CFT/CPF programmes or the group's business or risk profile.

Where gaps are identified through the gap analysis, Supervised Firms must take appropriate steps to address those gaps by amending its AML/CFT/CPF programmes as necessary, subject to any legislative or regulatory limitations in the jurisdictions in which other group entities operate.

Group-wide policies and procedures should be appropriate to all branches and majority-owned subsidiaries of the firm and must include, at a minimum:

- policies and procedures for sharing information required for the purposes of conducting CDD;
- AML/CFT/CPF risk management policies and procedures; and
- adequate safeguards governing confidentiality, security and permitted use of information exchanged, including safeguards to prevent tipping-off.

Consistent with firm procedures, group-wide AML/CFT/CPF policies and procedures should be regularly reviewed and kept up to date. Firms should maintain written records evidencing:

- the conduct and outcome of reviews and gap analyses;
- any amendments made to group-wide policies and procedures; and
- the steps taken to communicate group-wide policies and any material changes to relevant employees

CHAPTER 5 – RISK-BASED APPROACH

5.1 Overview of the Risk-Based Approach

Supervised Firms are exposed to the risk of being used, whether knowingly or unknowingly, to facilitate ML/TF/PF. Such risks may arise across a broad range of legal services, transactions, and business relationships and if unidentified and unmonitored may result in criminal liability, regulatory enforcement action, civil consequences, and significant reputational harm.

The RBA is a core principle underpinning the AML/CFT/CPF framework. It requires Supervised Firms to identify, assess, understand, and mitigate ML/TF/PF risks in a manner that is proportionate to the nature, size, complexity, and risk exposure of their practice.

Under the RBA, Supervised Firms:

- may apply simplified measures where risks are lower, where permitted by the AMLRs, but not whenever there is a suspicion of ML/TF/PF; must apply enhanced measures where ML/TF/PF risks are higher; and
- should efficiently allocate resources to ensure that risks are mitigated effectively.

The RBA supports effective compliance by enabling firms to focus attention and resources on higher-risk areas and applying proportionate compliance measures in lower-risk situations.

The RBA does not apply to TFS and the obligation to report suspicious activity. Once a suspicion of ML/TF/PF has been formed, reporting obligations under the POCA, the TA, and the PFPA apply irrespective of any assessed risk level. However, the RBA plays a critical role in the ongoing monitoring of client relationships and matters. It also assists Firms in identifying suspicious activity at an early stage.

In assessing ML/TF/PF risks within legal practices, there are three interrelated levels of risk assessments that Supervised Firms should conduct as part of an integrated AML/CFT/CPF framework:

- BRA, which evaluates the risks faced by the practice as a whole and is central to the firm's AML/CFT/CPF framework, informing the policies, procedures, and controls implemented across the practice;
- Client risk assessments, which identify and assess ML/TF/PF risks at the individual client level; and
- Matter risk assessments, which focus on risks arising from specific instructions or matters, particularly where those risks are novel, non-routine, or non-repetitive.

5.2 Business Risk Assessments

In accordance with regulation 8(1) of the AMLRs, Supervised Firms must take steps that are appropriate to the nature, size, and complexity of their practice to identify, assess, and understand the risks of ML/TF/PF to which they are exposed.

A BRA is the foundation of a firm's AML/CFT/CPF framework. It provides an overarching assessment of the risks faced by the practice as a whole and informs the design, implementation, and operation of the Supervised Firm's policies, procedures, and internal controls.

5.2.1 Scope of the BRA

When conducting a BRA, Supervised Firms must assess ML/TF/PF risks arising in relation to:

- the nature and profile of their clients;
- the countries or geographic areas in which clients reside, operate, or to or from which financial transactions occur;
- the legal services, and transactions offered by the Supervised Firm; and
- the delivery channels through which legal services are provided.

These risk categories should be considered collectively, as risks often arise from the interaction of multiple factors rather than in isolation.

5.2.2 Governance, Documentation and Review

Supervised Firms must ensure that their BRA is properly documented, kept up to date, and made readily available upon request by LSSA. The BRA should clearly record the Supervised Firm's assessment of inherent risks, the mitigating controls in place, and the resulting residual risk.

In conducting the BRA, Supervised Firms must take appropriate steps to identify, assess, and understand the ML/TF/PF risks they face, and must consider all relevant risk factors before determining their overall risk exposure. Supervised Firms must also ensure that they have documented policies, procedures, and controls that enable them to manage, monitor, and mitigate effectively the risks identified.

The BRA should be approved by senior management. Responsibility for ownership, approval, and periodic review of the BRA should be clearly assigned and documented. The Supervised Firm's risk appetite should be clearly defined, communicated and set at the appropriate level to ensure that risk decisions and mitigation measures are consistently applied across the practice.

The BRA should be treated as a living document. At a minimum, it should be reviewed annually and prior to material changes to the practice, including changes to services offered, client base, geographic exposure, delivery channels, ownership or management structure, the introduction of new technologies or applicable legal or regulatory requirements. The BRA should also be reviewed where emerging risks are identified through client or matter risk assessments or internal reviews.

5.2.3 Inherent Risk, Controls and Residual Risk

In accordance with regulation 8(2)(b) of the AMLRs, Supervised Firms must consider all relevant risk factors before determining both the overall level of ML/TF/PF risk faced by the practice and the appropriate level and type of mitigation to apply.

This requires Supervised Firms to distinguish clearly between:

- inherent risk, being the level of ML/TF/PF risk present before the application of any controls;
- mitigating controls, including policies, procedures, systems, and staff training et al; and
- residual risk, being the level of risk remaining after controls have been applied.

Residual risk should be understood and documented and should remain within the Supervised Firm's defined risk appetite. Where residual risk is assessed as exceeding appetite, Supervised Firms should implement additional controls or, where permitted and appropriate, consider declining or terminating the client relationship, with the decision clearly recorded.

5.2.4 New Products, Services and Technologies

In accordance with regulation 9 of the AMLRs, Supervised Firms must ensure that, prior to the introduction or use of any new product, service, business practice, delivery mechanism, or technological development, they identify and assess any ML/TF/PF risks that may arise. This includes risks associated with new delivery channels, systems, or the use of new or developing technologies in relation to both new and existing products or services.

Appropriate and proportionate mitigation measures should be implemented and approved before such products, services, or technologies are launched or adopted.

5.2.5 Information Sources Informing the BRA

In identifying and assessing ML/TF/PF risks, Supervised Firms should consider all relevant and available information. This information should be reviewed periodically and may include, but is not limited to:

- the Cayman Islands NRA;
- guidance and reports from international standard setting bodies such as FATF;
- guidance and reports issued by the FRA;
- legal sector risk assessments and thematic publications issued by the LSSA;
- publications, guidance, and notifications issued by the LSSA; and
- any other material relevant to the firm's risk profile, such as credible media reports highlighting risks in particular jurisdictions or sectors.

5.2.6 Client Risk

Certain characteristics or behaviours may increase the level of risk associated with a Supervised Firm's client base and should be reflected in the BRA.

Indicators of higher client risk may include reluctance to provide required information or documentation, reasonable grounds to suspect that information provided is inaccurate or insufficient, significant business activities or affiliations in higher-risk jurisdictions, complex or opaque ownership or control structures, political exposure, and unexplained or disproportionate wealth or funds, inter alia.

In assessing client-related risks at the business level, Supervised Firms should consider the overall composition of their client base, including whether clients are individuals or legal persons, whether ownership and control structures are readily identifiable, whether corporate clients are regulated and subject to equivalent AML/CFT/CPF obligations, and whether client information can be reliably verified.

Supervised Firms should have a good understanding of the following to make an informed assessment of their client risks:

- Who are your clients? Are they generally high risk?
- Are your clients mostly natural persons or legal persons?
- If they are legal persons, is the ultimate beneficial owner clearly identifiable? Or is the ownership structure complex?
- Do the clients reside locally or overseas?
- Are any clients identified as PEPs? Or are they close associates or family members of PEPs?
- Are any clients identified as HNWIs or UHNWIs?
- Have any clients been identified or suspected of illegal/criminal activity?
- Are clients active in higher-risk sectors (for example, cash-intensive businesses, virtual assets, charities, extractives, oil and gas), and does that activity affect the Supervised Firm's risk exposure?

5.2.7 Product/Services Risk

Certain legal services have been identified as presenting a higher potential ML/TF/PF risk, including the misuse or abuse of client accounts, real property transactions, the creation and management of trusts, companies, and charities, the management of assets, and sham or abusive litigation.

The provision of these services does not automatically render a practice high risk. However, Supervised Firms should assess these activities in the context of their overall practice and consider whether additional controls are required, particularly where such services are combined with higher-risk clients, jurisdictions, or transaction types. Supervised Firms should also consider risks arising from unusually complex or atypical mandates and ensure that staff are trained to identify relevant warning signs.

Supervised Firms should have a good understanding of the following to make an informed assessment of their product/services risks:

- What services does the Supervised Firm offer?
- Do the services offered carry a higher-risk of ML/TF/PF?
- What is the proportion of RFB work to non-RFB work?
- Do services involve the use of the Supervised Firm's client account, and if so, are there heightened risks of misuse or layering that require additional controls?
- Does the service involve the creation, administration, or management of companies, trusts, foundations, or similar structures that could be used to obscure beneficial ownership or control?

5.2.8 Geographical Risk

Geographic risk refers to the countries or geographic areas in which the Supervised Firm operates, receives funds from, carries out transactions or where clients reside. It may also extend to social, cultural or language ties that increase links to a known higher-risk jurisdiction.

Supervised Firms should consider whether:

- Clients or applicants for legal services reside in or money comes from sanctioned countries;
- The countries where legal services are offered follow and implement international rules and standards adopted to fight ML/TF/PF; or
- High levels of corruption and criminal activity exist in those countries.

Supervised Firms should carefully consider the jurisdictions in which they offer services and whether there are any particular local issues, of which they ought to be aware, which may impact their risk assessment.

Country risk factors should feature prominently in the assessment of the ML/TF/PF risks faced by Supervised Firms. Where clients or beneficial owners are based in, or operate their business in, higher-risk jurisdictions, this should be reflected in the BRA and in client and matter risk assessments as appropriate.

Higher-Risk Jurisdictions

When assessing ML/TF/PF risk, Supervised Firms must consider whether a client, transaction, or matter has a connection to a higher-risk country or geographic area. In accordance with regulation 8A, Supervised Firms should base their assessment on credible and authoritative sources when determining the level of risk associated with a country or geographic area. These sources include evaluations, assessment reports, follow-up reports, and public statements issued by recognised international bodies such as:

- the FATF and the CFATF;
- International Monetary Fund;
- World Bank;
- Organisation for Economic Co-operation and Development;
- the UN; or
- Any SA, CA or government body designated by Cabinet.

A country or geographic area must not be assessed as low risk where one or more of the following factors are present:

- The jurisdiction has been identified by credible sources as lacking effective systems to counter ML/TF/PF;
- The jurisdiction is identified as having significant levels of corruption, terrorism or ML/TF/PF;
- The jurisdiction is subject to sanctions imposed by the United Kingdom or the UN relating to ML/TF/PF risk;
- The jurisdiction has been identified by the FATF on either of the following lists:
 - Jurisdictions under increased monitoring;
 - High-risk jurisdictions subject to a call for action; and

- The jurisdiction is subject to an Order made under section 201(3) of the POCA; i.e. the jurisdiction has been designated by Cabinet as one with serious deficiencies in its compliance with recognised international standards for AML/CFT/CPF.

Some indicators of higher-risk jurisdictions include countries that:

- have deficient AML/CFT/CPF legislation, systems and practices and/or inadequate AML/CFT/CPF supervision;
- have high levels of acquisitive crime or higher levels of corruption;
- have a prevalence in the production of drugs, drug trafficking/trade or terrorism;
- are considered tax havens offering secretive tax regimes and low financial transparency;
- permits nominee shareholders to appear on the share certificate or register of owners; or
- have local requirements around company structure or equivalent governance which are unclear or otherwise make it challenging to understand the control structure of an entity.

Where a Supervised Firm's clients or the beneficial owners of those clients are based or operate their business in lower risk jurisdictions this should also be reflected in the BRA.

It is also important to consider whether the Supervised Firm is involved in multi-jurisdictional matters. Money launderers and terrorist financiers are commonly attracted to mechanisms which move money or value across borders, in order to obscure ownership and frustrate investigations.

If Supervised Firms do not have the ability or expertise to effectively assess the risk posed by a particular jurisdiction, they should consider whether it is appropriate to continue acting in relation to clients or matters associated with those jurisdictions.

Where higher-risk jurisdictions are identified, Supervised Firms must apply EDD measures proportionate to the nature and level of risk. This includes increased scrutiny of SoW and SoF, heightened ongoing monitoring, and a clear understanding of the purpose and legitimacy of the client relationship or transaction. Connections to such jurisdictions should be considered alongside other risk factors, including client type, service risk, and transaction risk, as part of an overall holistic risk assessment.

5.2.9 Transactions Risk

Supervised Firms should consider the types of transactions they facilitate, particularly with regard to the complexity and the risk that there may be parties to the transaction that they are not able to identify.

This is a potentially complicated area of risk and Supervised Firms should identify the most common transaction types undertaken by the Supervised Firm and describe how transactions falling outside those typical scenarios are assessed and rated.

For example, the Supervised Firm may want to set out the common range of values for the transaction that they are normally involved with, and other characteristics, for example, residential conveyancing transactions in a certain area. The Supervised Firm should set out the risks involved with this activity and any other common areas of practice and consider what the risk levels may be for activities that fall outside of these clearly assessed areas.

Supervised Firms should have a good understanding of the following to make an informed assessment of their transaction risks:

- What is the value or size of the transaction?
- Does the transaction involve multiple parties and jurisdictions?
- Does the transaction make economic sense?
- Is the transaction structured in a way that is unnecessarily complex, opaque, or difficult to understand, particularly when compared to its stated purpose?
- Is the transaction consistent with the client's known profile, SoW and business activities?
- Does the transaction involve unusual payment methods, including cash or virtual assets, or requests for third-party funding without a clear rationale?

5.2.10 Delivery Channels

Supervised Firms must consider the inherent risks associated with how they deliver their services. Supervised Firms should consider the percentage of their business that is conducted on a non-face-to-face basis and whether the practice undertakes work that is conducted through intermediaries or other third parties.

The manner in which Supervised Firms deliver their services should be considered when assessing risks and should include:

- the proportion and characteristics of clients that it does not meet face-to-face or do not verify with robust electronic identification and verification;
- how many of its matters rely on indirect contact with its client (for example, via a representative or agent) rather than holding a direct relationship with the client;
- how much of its activity is delivered online or via any other channel that may facilitate anonymity; and
- the methods used to undertake identification and verification and general due diligence requirements, and whether these are appropriate for the delivery model.

5.3 **Application of Risk Assessments**

BRAs should indicate the Supervised Firm's assessment of its inherent risks, the policies, procedures and controls implemented to mitigate the identified risks and residual risks that remain after considering the effectiveness of those mitigating measures. Comprehensive documentation of inherent risks, applicable policies and procedures, control activities, and residual risks promotes consistency, supports effective review and challenge, and facilitates timely updates and ongoing risk management.

Supervised Firms may choose to rate risks using a structured scoring system or a narrative approach. Regardless of methodology, consistency across risk categories is essential to ensure effective risk management. Risk assessments must not be treated as a tick-box exercise and are only effective if they actively inform client and matter-level decisions and the Supervised Firm's policies, procedures, and controls.

The assessed risk rating should determine the level of CDD applied (including whether EDD is required) and the frequency and intensity of ongoing monitoring. Findings of the BRA should be communicated to relevant staff and should be used to inform client acceptance, matter acceptance, and ongoing monitoring decisions.

It is not expected that Supervised Firms will eliminate all AML/CFT/CPF risk. However, Supervised Firms must ensure that the controls adopted are appropriate in light of the risks identified. Comprehensive, well-documented BRAs, client and matter risk assessments, and clear decision-making records enable Supervised Firms to demonstrate compliance to supervisors, law enforcement, and the courts, while protecting the practice from abuse.

5.4 Client Risk Assessments

This section explains how the firm-wide risk considerations are applied at the individual client level.

Supervised Firms must record a client risk assessment for every client for whom/which they carry out relevant financial business. Client risk assessments are a critical component of the RBA and must be informed by, and aligned with, the firm's BRA.

When undertaking a client risk assessment, Supervised Firms should consider which of the risk factors identified in Section 5.2 are relevant to the particular client. Particular attention should be paid to clients or relationships that the BRA identifies as having inherently higher-risk, as well as to situations where risks arise that are not fully addressed by the existing BRA. Where new or previously unidentified risks emerge at the client level, firms should consider whether the BRA requires reviewing or updating to ensure that those risks are appropriately reflected at the firm level.

An initial client risk assessment should be completed at the outset of the client relationship and should be conducted in conjunction with the application of CDD measures. However, Supervised Firms should recognise that a client's risk profile may evolve over time. In some cases, information relevant to assessing risk may only become apparent as the relationship develops or as specific matters progress.

Client risk assessment procedures should therefore be dynamic and ongoing. Information obtained while acting for a client, including changes in behaviour, instructions, ownership, source of funds, or transaction patterns, should feed back into the client risk assessment and, where relevant, the matter risk assessment.

The better a Supervised Firm understands its client and the nature and purpose of the instructions received, the better placed it will be to assess risk accurately, identify unusual or suspicious activity, and protect the business from abuse.

A fundamental element of any client risk assessment is an evaluation of whether the client's financial circumstances, business activities, SoW, and SoF are consistent with the client's overall profile and background. These considerations should be clearly documented within the client risk assessment and, where relevant, the matter risk assessment.

In assessing client risk, firms should consider a range of additional factors, including whether the structure, complexity, or nature of the client entity or relationship makes it difficult to identify ultimate beneficial owners or controlling interests, or whether the client appears to be attempting to obscure an understanding of their business, ownership, or the nature of their matters. Political exposure is also a key consideration, including whether the client is a PEP or a family member or known close associate of a PEP.

This list of considerations is not exhaustive. Where clients are regulated for AML purposes or are listed on a recognised stock exchange, this may provide some mitigation and comfort, although it does not remove the need for an appropriate and documented risk assessment.

Supervised Firms should also assess whether adverse or negative media coverage exists in relation to the client. Media checks may range from basic internet searches to more in-depth reviews, depending on the level of risk identified. In evaluating adverse information, firms should consider the reliability and credibility of the source, the seriousness and relevance of the allegations, and their timing.

Confidence in the outcome of any adverse media review depends on the quality of the underlying CDD. Firms should therefore ensure that CDD information is reliable and sufficient to identify and verify the client before placing reliance on conclusions drawn from media checks.

Some client risks will only become apparent when viewed in conjunction with the type of services or matters undertaken. Unusually complex matters, matters lacking an obvious economic or legal purpose, or matters that are otherwise atypical should be treated as risk indicators. Supervised Firms should ensure that staff are trained to identify such warning signs and that this training forms part of the mitigating controls documented in the BRA.

5.5 Matter-Level Risk Assessments

Matter-level risk assessments should focus on the specific risks presented by an individual instruction or transaction, over and above the client-level risks already identified.

It may not be necessary to complete a separate written matter risk assessment for every matter. A standalone matter risk assessment is less likely to be required where matters for a particular client are repetitive in nature, the risk profile remains consistent, and those risks are comprehensively addressed by the client risk assessment. Similarly, where a firm provides an ongoing registered office or similar service, a separate matter risk assessment may not be required for each instance, although ongoing monitoring of the relationship remains essential.

Matter risk assessments assist Supervised Firms in determining whether they are comfortable acting on a matter and whether continued involvement remains appropriate as it progresses. They also help identify whether adjustments to internal controls or due diligence measures are required. Where a matter is assessed as higher-risk, Supervised Firms will need to enhance monitoring, apply EDD, or impose additional internal oversight measures.

Both client-level and matter-level risk factors should be considered when assessing a specific matter. Matter risk may be elevated where the size, nature, purpose, commercial rationale, or complexity of the instruction is unusual or unclear, where the SoW or SoF is obscured, or where third parties are involved without a clear or logical relationship to the transaction. Difficulties in identifying beneficiaries, ownership interests, control structures, or transactions structured in a way that obscures their true nature, may also indicate heightened risk. Risk may also arise where the matter does not align with the client's known profile or involves sectors in which the client would not ordinarily operate.

Matter risk assessments should record the relevant circumstances, identify the risks with reference to the BRA, assign an overall risk level, and provide a clear rationale for that assessment.

5.6 Risk Weightings

When applying risk weightings, Supervised Firms should take a holistic approach and exercise informed professional judgement in assessing the relevance, interaction and impact of different risk factors in the context of a particular client or matter. Many Supervised Firms use scoring systems or matrices to assist with this process; however, care should be taken to ensure that cumulative scoring does not inadvertently dilute serious risks when offset by lower-risk factors.

Supervised Firms should consider whether certain factors should act as automatic high-risk triggers, such that a client or matter is classified as high risk regardless of any numerical score achieved. Where either the client or the service provided presents a higher level of risk, it may be appropriate to treat the overall matter as high risk.

Any deviation from established scoring outcomes or methodologies should be clearly documented, with reasons recorded either on a matter-by-matter basis or within the BRA. Weighting approaches should not be influenced by commercial considerations or a desire to retain profitable relationships, should not prevent any client or matter from being classified as high risk, and should avoid unintended consequences where significant risks are inappropriately outweighed by lower-risk factors.

Where a Supervised Firm assesses a particular risk differently from the NRA or supervisory guidance, this should be clearly justified and documented in the BRA, taking into account the Supervised Firm's specific mitigating controls. However, where lower risks identified by the firm are not commensurate with the NRA, SDD should not be applied.

An overall risk conclusion must always be reached after all relevant factors have been considered, before determining the appropriate level of mitigation to apply.

5.7 Documenting Risk Assessments

There is no prescribed format for recording risk assessments; however, all assessments must be documented in writing and capable of being produced to the Supervised Firm's supervisor or other CA upon request.

Risk assessment records must demonstrate that all relevant factors have been considered and should clearly indicate the reasoning and methodology applied. Each assessment must record the overall risk level assigned and should be signed and dated, whether manually or electronically, by the individual responsible for conducting or approving the assessment.

Documentation must be maintained to provide a clear and reliable record of risk assessment decisions, including any changes to risk ratings and the rationale for those changes. Risk assessment records should be kept up to date and reviewed as necessary to reflect material changes in client circumstances, matters, or risk exposure.

5.8 Risk Mitigation

Risk mitigation involves the process of implementing policies, procedures and other control measures to manage the ML/TF/PF risks identified. Supervised Firms should ensure that the policies, procedures and controls implemented are in line with the level of risk identified, consistent with any legal or supervisory requirements and are approved by senior management of the firm.

Where a client or matter is assessed as higher-risk, Supervised Firms must apply proportionate and effective measures to mitigate the identified ML/TF/PF risks. Mitigation measures should be tailored to the specific risks present and may include EDD, increased scrutiny and frequency of ongoing monitoring, escalation procedures, restrictions on the scope of services provided or the imposition of additional internal controls.

The presence of a single risk factor, or even multiple risk factors, does not necessarily indicate that a client is engaged in ML/TF/PF activity. Supervised firms should exercise sound informed professional judgement when evaluating risk indicators in context. However, where a combination of factors gives rise to heightened concern, Supervised Firms should ensure that appropriate escalation, additional controls, or decisions to decline or discontinue the relationship are considered and clearly recorded.

Supervised Firms must maintain documented policies and procedures that set out how risk mitigation measures are selected, applied, and escalated in response to assessed risk levels, including the circumstances in which services may be restricted, refused, or terminated.

5.9 Monitoring of Controls

In accordance with regulation 8(2)(e) of the AMLRs, Supervised Firms must assess the effectiveness of the risk mitigation policies, procedures or controls implemented and identify and enhance any areas requiring improvement.

Firms should ensure that risk mitigation measures are designed appropriately to address the ML/TF/PF risks which they purport to manage. In addition, firms should periodically test these mitigating measures to ensure that they are operating as intended.

CHAPTER 6 – CLIENT DUE DILIGENCE

6.1 Purpose and Scope of Client Due Diligence

CDD is a fundamental preventive measure under the AMLRs and is central to protecting Supervised Firms from being misused for ML/TF/PF.

CDD is a holistic process and is not limited to the identification and verification of a client's identity. It encompasses a range of measures designed to enable a Supervised Firm to understand:

- who the client is and, where relevant, on whose behalf the client is acting;
- the ownership and control structure of non-natural persons;
- the purpose and intended nature of the business relationship or transaction; and
- the origin of funds and, where appropriate, the origin of a client's overall wealth.

The nature, extent, and depth of CDD measures applied must be risk-based, proportionate, and commensurate with the ML/TF/PF risks identified through the BRA, and the client/matter risk assessments.

Supervised Firms must be able to demonstrate to LSSA that the CDD measures applied are appropriate and effective in mitigating identified risks. This includes maintaining clear and accurate records of the rationale for decisions taken and measures applied.

CDD is not a static or purely procedural exercise. It requires the exercise of professional judgement and an informed assessment of whether the legal services being provided are consistent with the Supervised Firm's understanding of the client, the transaction, and the associated risk profile.

CDD policies, controls, and procedures must be clearly documented, communicated, consistently applied, and accessible to all relevant staff. Supervised Firms should ensure that employees understand both the regulatory requirements and the underlying purpose of CDD as a key safeguard against ML/TF/PF risks.

6.2 CDD Framework

The AMLRs require Supervised Firms to establish and maintain a comprehensive CDD framework forming part of their policies, controls and procedures.

The CDD framework must be applied on a risk-based and proportionate basis, having regard to the firm's BRA and the specific risks associated with the client, the matter and the transaction. The framework should include:

- a) Procedures for the identification and verification of natural persons, using reliable and independent sources;
- b) CDD processes, including procedures to identify and understand the ownership and control structures of legal persons and legal arrangements;
- c) Processes for identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity;

- d) Measures to verify that a person purporting to act on behalf of a client is properly authorised and identify and verify the identity of the person;
- e) Measures to obtain and understand information on the purpose and intended nature of the business relationship or transaction;
- f) Processes for conducting ongoing due diligence throughout the business relationship;
- g) Procedures to assess and document the client's SoF and SoW, with the nature and extent of evidence aligned to the client/matter risk profile;
- h) EDD controls for higher-risk clients and transactions, including appropriate measures in respect of SoF and SoW where required;
- i) The application of SDD, where permitted under the AMLRs; and
- j) Processes for identifying PEPs, their family members and close associates, and managing the associated risks.

Not all CDD measures will be required in every case. The nature, timing and extent of CDD applied must be appropriate to the level of ML/TF/PF risk identified.

6.3 When CDD is Required

Pursuant to regulation 11 of the AMLRs, Supervised Firms are required to apply CDD measures in the following circumstances:

- When establishing a business relationship;
- When carrying out a one-off transaction with a value exceeding CI\$10,000, whether executed as a single transaction or as several transactions that appear to be linked;
- When carrying out a one-off transaction that is a wire transfer;
- Where there is a suspicion of ML/TF/PF; or
- Where there are doubts about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

These obligations apply irrespective of any exemptions or thresholds that may otherwise be available.

6.3.1 Business Relationship

In determining whether a business relationship is being established, Supervised Firms should assess the substance of the arrangement at the point instructions are accepted, having regard in particular to whether:

- the instructions contemplate an ongoing or a repeated course of dealing, rather than a single isolated transaction;
- the services are expected to be provided over a period of time; and
- the overall value of payments to be made under the arrangement cannot be determined at the outset.

This definition should be interpreted broadly. In practice, it is reasonable to assume that a business relationship is formed whenever a Supervised Firm accepts instructions from a client for the first time,

unless there are clear and documented reasons to conclude that the engagement is genuinely limited to a single, isolated service with no expectation of duration.

6.3.2 One-Off Transactions

A one-off transaction is any transaction that is not carried out in the course of an established business relationship, as defined in regulation 2 of the AMLRs.

In the legal sector, a one-off transaction typically refers to a single, discrete service provided at a specific point in time, with no expectation of an ongoing relationship.

CDD must nevertheless be applied where a one-off transaction has a value exceeding CI\$10,000, whether carried out as a single transaction or as a series of linked transactions. For these purposes, the value relates solely to the sums involved in the transaction(s) and does not include legal fees or distributions. The CI\$10,000 threshold does not determine whether an instruction is a one-off transaction or a business relationship. It applies only after the instruction has been properly classified as a one-off transaction. For example, where a Firm provides a genuinely discrete, one-time service involving the transfer of an asset, with no continuing duties or expectation of further services, the instruction may constitute a one-off transaction. The Firm's legal fees and disbursements are not included when calculating that value. CDD must also be applied irrespective of the value of the transaction where there is a suspicion of ML/TF/PF, other criminal conduct or doubt about the veracity or adequacy of previously obtained client identification data.

Given the nature of legal services, genuinely one-off transactions are expected to be uncommon, and Supervised Firms should exercise caution before concluding that a business relationship has not been formed. In determining whether an instruction constitutes a one-off transaction, a Supervised Firm should consider the substance and surrounding circumstances of the engagement and not merely its duration, value or description. An instruction should not be treated as one-off merely because it is completed quickly, concerns a single matter, is below CI\$10,000 or is the Firm's first or only instruction from the client. Where the work involves continuing professional duties, implementation or completion steps, the holding or management of client assets, follow-up advice, linked instructions, or a reasonable expectation of further services, a business relationship will ordinarily have been established. Any determination that an instruction is a one-off transaction should be supported by the engagement terms or other information held by the Supervised Firm. Where there is doubt, the Firm should treat the instruction as establishing a business relationship and apply CDD accordingly.

6.3.3 Suspicion, About Existing CDD

In addition to the circumstances set out above, the AMLRs require Supervised Firms to apply, or reapply, appropriate CDD measures where the Supervised Firm has a suspicion of ML/TF/PF; or the Supervised Firm has doubts about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

In such circumstances, Supervised Firms must take appropriate steps, on a risk-sensitive basis, to review and update CDD information and to assess whether the relationship or transaction remains consistent with the Supervised Firm's understanding of the client, the matter, and the associated risk profile. Supervised Firms must ensure that documents, data and information collected under CDD are kept current and relevant, giving consideration to the adequacy of the data obtained.

Where suspicion arises, Supervised Firms should have regard to the risk of tipping off and must act in accordance with their legal and regulatory obligations.

6.3.4 Examples of Suspicion of ML/TF/PF

Examples of circumstances that may give rise to a suspicion of ML/TF/PF include, but are not limited to:

- a client is unwilling, evasive or inconsistent when asked to explain the purpose of the instruction, the SoF or the SoW;
- the transaction or structure appears unnecessarily complex, opaque or disproportionate to the stated purpose, and no credible commercial or legal rationale is provided;
- funds are received from, or intended to be transferred to, third parties with no apparent connection to the client or the matter;
- the client seeks to proceed with urgency or applies pressure to complete a transaction before CDD measures can be completed, without a reasonable explanation;
- the value or nature of the transaction appears inconsistent with the client's known background, profession, business activities or financial circumstances;
- the client seeks to use the Supervised Firm's client account in a manner that appears to facilitate the movement of funds without a clear underlying legal service; or
- information obtained during CDD or the matter suggests possible links to criminal activity, corruption, sanctions exposure, or high-risk jurisdictions without a credible explanation.

6.3.5 Doubts as to the Veracity or Adequacy of Documents, Data or Identification Documentation

Examples of circumstances that may give rise to doubts about the veracity or adequacy of documents, data or identification information previously obtained include, but are not limited to:

- identification documents appear altered, forged, expired, damaged, or otherwise unreliable;
- inconsistencies arise between information provided by the client and information obtained from independent or reliable sources (such as registries, databases or public records);
- the client provides different versions of personal details (such as name, date of birth, address or nationality) without a satisfactory explanation;
- discrepancies are identified in ownership or control information, including inconsistencies between information obtained through CDD and information held in official registers;
- documents provided are incomplete, lack required certification, or are issued by a source whose reliability cannot be reasonably established;
- the client fails or refuses to provide updated documentation when requested, or provides documents that do not adequately address the Supervised Firm's CDD requirements; or
- the Supervised Firm becomes aware that documents or information relied upon for CDD purposes are no longer current or may have changed since they were obtained.

6.4 Components of CDD

CDD comprises a number of interrelated and ongoing measures which, taken together, enable a practice to understand with whom it is dealing, the purpose and nature of the business relationship, and the risks associated with the instructions it is asked to undertake.

In accordance with the AMLRs, CDD consists of the following core components:

- identification of the client;
- verification of the client's identity;
- identification and verification of any person acting on behalf of the client;
- identification and verification of any beneficial owner, natural person exercising control of the legal person or arrangement or senior managing official;
- obtaining information on the purpose and intended nature of the business relationship; and
- conducting ongoing monitoring of the business relationship. (Ongoing monitoring will be addressed in Chapter 7).

These components must be applied on a risk-based basis and to a standard that is proportionate to the risks presented by the client, the transaction, and the nature of the services provided.

6.4.1 Identification of the Client

Identification involves establishing the client's identity by obtaining their key identifying details. For a natural person, this will normally include their full name, date of birth, nationality, and residential address. For a legal person or legal arrangement, this will include its legal name, legal form, registration number, registered office, and principal place of business.

Identification is the process by which the Supervised Firm is told, or comes to know, who the client is. It precedes verification and must be completed before any attempt is made to confirm the client's identity.

Where the client is not a natural person, the Supervised Firm must also identify the relevant individuals who control or direct the entity and those who purport to act on its behalf.

6.4.2 Verification of Identity

Verification is the process of confirming that the identity claimed by the client is true, by reference to documents, data or information obtained from a reliable source which is independent of the client.

Verification must be sufficient to enable the Supervised Firm to be satisfied that it knows who the client is. The nature and extent of verification required will depend on the client's risk profile, the nature of the relationship, and whether the client is physically present for identification purposes.

Verification may be undertaken using:

- original documents or certified copies;
- electronic or digital verification systems;
- information obtained from other regulated persons; or
- reliable and independent public sources.

Verification must be completed in accordance with the timing requirements set out in this chapter and recorded in a manner that enables the Supervised Firm to demonstrate compliance.

6.4.3 Persons Acting on Behalf of Clients

In accordance with regulation 12(1)(b), where a person purports to act on behalf of the client, the Supervised Firm must identify and verify the identity of the person acting and must take reasonable steps to confirm the existence and scope of their authority to act for the underlying client.

Supervised Firms must take reasonable steps to understand the nature and scope of the authority relied upon, including by obtaining and reviewing appropriate documentary evidence such as powers of attorney, board resolutions, letters of appointment, or equivalent instruments.

Authority to instruct may be evidenced through an engagement letter or equivalent document, but such authority should originate from the underlying client, including where instructions are given through an employee of a corporate client.

Even where a person does not explicitly purport to act on behalf of another, Supervised Firms should consider whether there may in fact be an underlying client who is the recipient of the services on an ongoing or repeated basis, including where instructions are channelled through another professional service provider.

Where this is a possibility, Supervised Firms must satisfy themselves that:

- the underlying client has been properly identified and their identity verified; or
- an appropriate reliance arrangement has been established with the professional intermediary in accordance with the AMLRs.

Supervised Firms must always be clear as to the identity of its client and the nature of the client relationship.

There may be circumstances in which the intermediary is the Supervised Firm's contractual client, but the intermediary's own client is the ultimate beneficiary of the work and advice provided. In such cases, the AMLRs make clear that a 'beneficial owner' includes the individual on whose behalf a transaction is being conducted. The Supervised Firm must therefore treat that individual as a beneficial owner and take reasonable measures to identify and verify their identity.

This is to be distinguished from a simple referral arrangement, where an entity refers a client to the Supervised Firm but does not act on the client's behalf in the transaction or matter.

Where the intermediary is a legal person, the Supervised Firm should consider, on a risk-sensitive basis, whether it is also necessary to identify and verify the ultimate beneficial owners of the intermediary.

6.4.4 Identification and Verification of Beneficial Owners

Regulation 12(1)(c) requires Supervised Firms to identify and verify beneficial owners.

Where the client is a natural person, that individual may ordinarily be treated as the beneficial owner, unless the features of the transaction or the surrounding circumstances indicate that the individual

may be acting on behalf of another person. In such cases, Supervised Firms must consider whether there is an underlying beneficial owner whose identity must be established.

In determining whether a client is acting on their own behalf, Supervised Firms should consider whether the services requested are consistent with what is known about the client and the nature of the instruction.

Where a Supervised Firm identifies a discrepancy between beneficial ownership information obtained through CDD measures and information held on an official register or other authoritative source, the Supervised Firm should take appropriate steps to resolve the discrepancy.

If the discrepancy cannot be reasonably explained or resolved, the Supervised Firm should assess whether this gives rise to a suspicion of ML/TF/PF and consider whether a SAR should be filed. Supervised Firms should also comply with any applicable beneficial ownership requirements to report discrepancies to the General Registry.

The identification of discrepancies, steps taken to resolve them, and the outcome of that assessment should be appropriately documented.

6.4.5 Purpose and Intended Nature of the Business Relationship

As part of CDD, Supervised Firms must assess and, where appropriate, obtain information on the purpose and intended nature of the business relationship or occasional transaction. This is a fundamental element of CDD and assists the Supervised Firm in assessing whether the relationship and any transactions conducted are consistent with the Supervised Firm's knowledge of the client.

Information obtained may include, where relevant:

- the nature of the client's business, occupation or activities;
- the reason the client is seeking the Supervised Firm's services;
- the anticipated type, volume and frequency of transactions or activity; and
- the expected duration of the business relationship.

The extent of information obtained should be commensurate with the ML/TF/PF risk presented by the client and the transaction. Supervised Firms should record their understanding of the purpose and intended nature of the relationship and use this information to inform ongoing monitoring.

6.5 Timing and Completion of CDD

6.5.1 General Timing Requirements

The ideal time to conduct CDD measures is prior to entering into a business relationship or carrying out a one-off transaction.

6.5.2 Delayed Verification

Regulation 15 of the AMLRs requires Supervised Firms to verify the identity of clients and their beneficial owners before or during the course of establishing a business relationship or conducting one-off transactions. Identity verification should be completed as early as possible so that Supervised Firms are satisfied that they know the identity of the client on whose behalf they are acting.

Where permitted by the AMLRs, a Supervised Firm may complete verification after the establishment of a 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 ML/TF/PF risks are effectively managed.

A Supervised Firm should consider its BRA when establishing the types of clients, matters and services for which delayed verification may be considered. It should adopt and document risk-management procedures specifying the conditions under which a client may use the business relationship before verification is completed.

The decision to delay verification in a particular case, the reasons for the delay, the deadline for completing verification, and the measures taken to manage the resulting risks, in alignment with the firm's risk management procedures, should be documented in the client/matter risk assessment, and be made available to the LSSA on request.

Before permitting delayed verification, the Supervised Firm should conduct all applicable CDD measures to determine the level of risk presented, as well as assess and document whether the conditions in Regulation 15 are satisfied and associated risks can be effectively managed. Delayed verification will generally be inappropriate where the client or matter presents a higher ML/TF/PF risk, unless the Supervised Firm can demonstrate that the risks can be effectively managed through enhanced and documented controls.

Supervised Firms should conduct CDD before substantive work is conducted for that particular client, funds are permitted to be deposited in the firm's client account unless they are for fees and disbursements, before property is allowed to be transferred or final agreements signed or completed.

If there is any delay in verification, Supervised Firms should ensure that an assessment is conducted prior to making this decision, as a client that is considered high risk may not be effectively managed in a way that would reduce the risk, thereby making this inappropriate. Therefore, the risk may be too high to allow any delay in verification.

6.5.3 Incomplete CDD

Where a Supervised Firm is unable to complete the required CDD measures, it must:

- not establish the business relationship;
- not carry out the transaction; and
- terminate any relationship that has already commenced.

In such circumstances, Supervised Firms must consider whether the failure to complete CDD gives rise to a suspicion of ML/TF/PF, and whether a SAR is required to be filed with the FRA.

6.5.4 Tipping-Off Considerations

The AMLRs prohibit tipping off. A risk may arise that, in seeking to complete CDD obligations or to obtain additional information where there is a suspicion of ML/TF/PF, a Supervised Firm may inadvertently alert a client to the existence of a possible SAR or investigation.

Any such awareness on the part of the client may compromise the effectiveness of subsequent investigative or enforcement action.

Accordingly, where a Supervised Firm forms a suspicion of ML/TF/PF in the course of conducting CDD, it should have regard to the risk of tipping off when deciding how to proceed. Where the firm reasonably believes that continuing the CDD process or making further enquiries would be likely to alert the client, it may decide not to pursue those enquiries and should consider making a SAR without delay.

Supervised Firms must ensure that all relevant employees are aware of, and sensitive to, the risk of tipping off when conducting CDD measures and are trained to manage such situations appropriately.

6.6 Methods of Identification and Verification

6.6.1 General Standard

Supervised Firms must identify the client, and where applicable any beneficial owner and any person purporting to act on behalf of the client, and must verify their identity using reliable, independent source documents, data or information.

Regulation 20 provides that evidence of identity of a client is satisfactory only where:

- it is reasonably capable of establishing that the client is who they claim to be; and
- the Supervised Firm is satisfied, in accordance with the procedures maintained under the AMLRs, that the evidence does establish that fact.

Where there is any doubt as to the accuracy, authenticity or adequacy of the evidence obtained, the Supervised Firm must obtain additional or alternative evidence until it is satisfied that the CDD requirements in accordance with the AMLRs have been met.

In determining whether evidence of identity is satisfactory, Supervised Firms should consider the nature of the relationship or transaction, the geographic risk factors involved, the practicability of obtaining evidence prior to commitment or payment, and the earliest point at which it is known or reasonably suspected that the CI\$10,000 threshold has been met, whether through a single transaction, linked transactions, or information arising at a later stage.

6.6.2 Identification and Verification of Natural Persons

The name, date of birth and current address of natural persons should all be identified and verified. The Supervised Firm must also obtain sufficient information to understand the nature of the proposed relationship.

The following information will normally be required:

- full legal name and any other names used;
- permanent residential address, including postcode where applicable;
- date and place of birth;
- nationality or nationalities;
- occupation or employment;

- the purpose of the business relationship, account or transaction;
- the estimated level and nature of activity expected; and
- the SoF, including the origin of the assets or income to be used in the relationship.

At a minimum, Supervised Firms must record the individual's full legal name, current address or place of business or employment, date of birth and nationality.

Where appropriate, and on the basis of risk, Supervised Firms may supplement documentary evidence with additional independent information, such as a reference from a respected professional with whom the client maintains a current relationship, or other suitable references.

Nationality must be established in order to determine whether the applicant is connected to a high-risk jurisdiction or a country subject to financial sanctions or other prohibitions.

Obtaining and recording a date of birth provides an additional safeguard, including where a forged or stolen document is presented bearing details that are inconsistent with the apparent age of the individual.

Documentation for Evidence of Identity

Information and documentation must be obtained and retained to support or confirm the details provided by the client.

Identification documents, whether originals, certified copies or, where permitted, legitimate electronic documentation, should:

- be pre-signed by the applicant;
- bear a clear photograph of the applicant; and
- be current, valid and unexpired.

Examples of acceptable primary identification documents include:

- a current valid passport;
- a government-issued photographic identity card; or
- a Cayman Islands provisional or full driving licence bearing the applicant's photograph and signature.

Documents which do not bear a photograph or signature, or which are easy to obtain, will not normally be appropriate as sole evidence of identity. Examples include birth certificates, credit cards, student cards and non-Cayman provisional driving licences.

Where documents are unfamiliar because of their origin, format or language, the Supervised Firm should take reasonable steps to satisfy itself that the document is genuine. This may include contacting the issuing authority or obtaining a notarised translation.

Where verification is conducted using photographs or videos processes,¹¹ the image should clearly show the client's face together with the identity document, in order to demonstrate that the document belongs to the applicant. A clear colour copy or scan of the identity document itself is also required to be obtained.

The use of video processes should be considered in accordance with a risk-based approach.

CDD documents received in electronic form are acceptable provided that the Supervised Firm adopts a proportionate approach and has documented policies and procedures in place to ensure the authenticity and integrity of the electronic documents.

Persons Without Standard Identification Documentation

It is recognised that certain categories of clients may be unable to produce standard forms of identification.

In such cases, a flexible and common-sense approach may be adopted, provided that the Supervised Firm remains satisfied that the individual's identity can be verified using alternative original or certified documents, preferably bearing a photograph.

Where the required information and documentation cannot be obtained, the Supervised Firm may seek confirmation of identity from another regulated institution or other person qualifying under the AMLRs. Failure to obtain a timely and positive response should be treated as a matter of concern.

Verification of Name and Address

The Supervised Firm must take appropriate steps to verify both the name and the address of the applicant. This may include one or more of the following methods:

- obtaining a reference from a respected professional who knows the applicant;
- checking the register of electors;
- making a credit reference agency enquiry;
- checking a current local telephone directory;
- inspecting a recent rates or utility bill, ensuring that the document is original or an original electronic issue; or
- conducting a personal visit to the applicant's residence where practicable.

For these purposes, a 'respected professional' may include lawyers, accountants, directors or managers of regulated institutions, ministers of religion, teachers, or other persons of standing.

Where an applicant's address is temporary accommodation, the Supervised Firm may accept alternative evidence such as a contract of employment, a lease agreement, or written confirmation from an employer or banker.

¹¹ Video Processes entails a visual method of communication between two or more remote parties over the internet for the purpose of identity verification.

Where an applicant appoints an additional account signatory or authorised person, full identification and verification procedures must also be applied to that person.

Certification of Identification Documents

Where certified copies are relied upon, the certifier must be a suitable person, such as a lawyer, accountant, notary public, director or manager of a regulated entity, a member of the judiciary or a senior civil servant.

The certifier must:

- certify the documents as true copies of the original documents and true likenesses of the individual;
- sign the copy document;
- clearly print their name and professional capacity;
- the date of certification;
- provide a contact address and telephone number; and
- where applicable, an official stamp or seal.

The Supervised Firm must satisfy itself that the certifier is appropriate and reliable, particularly where documents originate from higher-risk jurisdictions or unregulated entities.

Face-to-Face and Non-Face-to-Face¹²

Where the client is met face-to-face, original documents should be inspected, copied, and certified by suitably trained staff.

Non-face-to-face relationships may present increased risk and should be subject to appropriate controls. Where original identification documents cannot be inspected, the Supervised Firm must verify the client's identity using reliable, independent source documents, data or information and apply verification measures proportionate to the risks identified. Such measures may include requiring appropriately certified copies, using a suitably reliable and independent digital identification system, validating information against independent sources, or applying other measures that provide an appropriate level of assurance. Where elevated risk is identified or where the available evidence provides insufficient assurance, the Supervised Firm should apply certification, or other additional verification measures appropriate to mitigate the identified risks.

In the case of non-face-to-face onboarding, the adoption of digital ID technologies for e-KYC¹³ should be risk assessed and considered within the context of an RBA. Supervised Firms should ensure that the assurance levels¹⁴ of these tools are adequate for the level of risk presented by the jurisdiction,

¹² Non-face-to-face refers to the establishment of a business relationship or the carrying out of a transaction where the client is not physically present at the place where the relationship is being established or transaction is conducted.

¹³ Electronic Know Your Client refers to the processes whereby a client's identity is verified via electronic means.

¹⁴ Assurance levels measure the level of confidence and accuracy in the reliability and independence of a digital ID system.

product, client and other relevant risk factors. In the case of higher-risk scenarios, Supervised Firms should consider conducting additional verification measures to ensure the accuracy of e-KYC procedures.

Supervised Firms that utilise video-conferencing¹⁵ as an e-KYC method for verifying the identity and authenticity of ID documents should apply appropriate controls and ensure such an approach is in accordance with the risk profile of the client/matter. In intra-group business, certification must comply with both group standards and the local regulatory requirements of the jurisdiction concerned and must be at least equivalent to the Cayman Islands standard.

6.6.3 Identification and Verification of Legal Persons and Legal Arrangements

Where the client is a legal person or legal arrangement, Supervised Firms must identify the entity, understand its ownership and control structure, and identify and verify the identity of any natural person who is a beneficial owner or who otherwise exercises control.

Supervised Firms must take reasonable measures to identify:

- any natural person/s who ultimately owns or controls the client; and
- where no such person can be identified, the natural person who exercises control through other means or who holds a senior management position exercising control over the entity.

Where no natural person is identified through ownership or control, the relevant senior managing official (such as a general partner, president, chief executive officer, director, manager, or equivalent) must be identified and verified as the controlling person.

Corporate Clients and Other Legal Persons

Supervised Firms must obtain sufficient information and documentation to:

- establish the legal existence of the entity;
- understand the nature of its business and the purpose of the relationship;
- identify and verify the beneficial owners; and
- identify and verify those authorised to act on its behalf.

Depending on the nature, structure and risk profile of the applicant, this will normally include:

- a certificate of incorporation or equivalent evidence of formation;
- details of the registered office and, where different, the principal place of business;
- an explanation of the nature of the business, the reason for the relationship, the expected level of activity and the SoF;
- a copy of the most recent financial statements, where appropriate;

¹⁵ Video-conferencing is live, visual and audio method of communication connection between two or more remote parties over the internet that simulates a face-to-face meeting.

- satisfactory evidence of the identity of each legal owner and beneficial owner, together with a register of members or equivalent record;
- evidence of the identity of all authorised signatories, together with details of their relationship to the entity;
- evidence of authority to enter into the relationship, such as a board resolution or equivalent mandate;
- copies of any powers of attorney or other authorities affecting the operation of the account or transaction;
- a list or register of directors or equivalent governing body;
- satisfactory evidence of identity for directors or senior managers, taking a proportionate approach to the number of individuals verified;
- a certificate of good standing or equivalent confirmation that the entity remains in existence; and
- a copy of the constitutional or governing documents, such as the memorandum and articles of association or by-laws.

Where account signatories are not directors, managers or employees of the entity, the Supervised Firm should exercise particular caution and ensure that both identity and authority are clearly established.

Where original constitutional or incorporation documents cannot be obtained, suitably certified copies may be accepted in accordance with the certification standards set out in this Chapter.

Supervised Firms who are unable to verify official constitutive documents presented during video-conferencing or via other electronic methods due to unavailability of public sources must seek alternative measures to verify the documentation.

The Supervised Firm should remain alert to the risk that corporate entities may be used to disguise the identity of the true beneficial owner and must take reasonable measures to ensure that it is not entering into a relationship with such entities.

Where the Supervised Firm provides registered office services to a private trust company, it must also obtain the identification evidence required for trust and fiduciary customers, save to the extent that such information has already been obtained.

Partnerships and Unincorporated Businesses

Supervised Firms should obtain:

- identification evidence for at least two partners or controllers, the general partner and any authorised signatories;
- evidence of the trading address and principal place of business;
- a copy of the most recent financial statements, where appropriate;
- an explanation of the nature and purpose of the business or partnership; and
- identification evidence for the underlying beneficial owner where nominee arrangements exist.

Where a formal partnership arrangement exists, a mandate or equivalent authority authorising the relationship and identifying those empowered to transact must be obtained.

Where authorised signatories change, the identity of the new signatories must be verified without delay.

Trusts and Other Legal Arrangements

Trusts and other fiduciary arrangements present particular risks of misuse and require careful scrutiny.

In the case of trusts, the Supervised Firm must identify and take reasonable measures to verify the identity of:

- the settlor;
- the trustees;
- any protector or enforcer;
- the beneficiaries, or where not yet determined, the class of beneficiaries; and
- any other natural person exercising ultimate effective control over the trust.

In the case of other legal arrangements, the Supervised Firm must identify persons holding positions equivalent to those listed above.

In addition to identifying trustees and authorised signatories, the Supervised Firm should normally:

- make appropriate enquiries into the nature and purpose of the trust and the SoF;
- obtain identification evidence for the settlor;
- where a nominee arrangement exists, obtain identification evidence for the underlying beneficial owner; and
- in the case of a private trust company, consider whether corporate client documentation should also be obtained, to the extent not already held.

Where it is impractical to obtain all information, or where additional information is required because of the risks identified, the Supervised Firm should take a proportionate approach and document the rationale for the level of enquiries made.

Non-Profit Organisations

Where the applicant is an NPO, the Supervised Firm must obtain sufficient information to understand:

- the nature, purpose and operations of the organisation; and
- the identity of at least two authorised signatories or persons giving instructions.

Where the NPO is incorporated or established as a trust, the relevant corporate or trust identification procedures must be applied.

Where the NPO is established overseas, the Supervised Firm should, where appropriate, verify its registration with the relevant supervisory or registry body and undertake reasonable searches to

ensure that the organisation does not appear on sanctions lists or is not associated with terrorist or criminal activity.

The Supervised Firm should undertake a proportionate vetting of foreign NPOs, including basic public source checks and verification of the identity of representatives and signatories.

Particular care should be taken where the activities or beneficiaries of the NPO are located in higher-risk jurisdictions.

6.7 Source of Funds and Source of Wealth

A fundamental element of CDD is obtaining an understanding of the nature, background and circumstances of the client, including their financial position, and assessing whether the legal services and transactions are consistent with that understanding.

The extent to which a Supervised Firm must obtain, review and evidence information about a client's financial position will depend on the risk profile of the client, the matter and the transaction. In higher-risk situations, and in particular where EDD is required, this obligation is more stringent. For these purposes, a client's financial circumstances are commonly considered under two related but distinct concepts: SoF and SoW.

A Supervised Firm must scrutinise transactions on a matter-by-matter basis with the objective of understanding the origin of the funds used for each transaction undertaken on behalf of a client. This is an important safeguard against the misuse of the Supervised Firm for money laundering or other financial crime.

The nature and reliability of the documentation obtained to verify SoF and SoW should be proportionate to the level of ML/TF/PF risk presented. The higher the risk, the more comprehensive and reliable the evidence obtained should be.

Supervised Firms must take adequate measures to establish SoF and SoW as part of EDD applied to PEPs and should consider doing so in other instances of EDD on a risk-sensitive basis.

It is also good practice to consider SoF checks even where a formal business relationship has not been established and the instruction relates to an occasional transaction. In all cases, the Supervised Firm must document the SoF and SoW enquiries undertaken, the information and evidence obtained, and the conclusions reached.

6.7.1 Source of Funds

SoF refers to the origin of the specific funds used to finance the transaction or activity in question.

The purpose of establishing SoF is not merely to identify the account from which the funds are transferred, but to understand how and from where the client obtained the money used for the transaction.

Merely identifying that funds have been transferred from a specific bank account is generally insufficient to satisfy SoF requirements.

Where the transaction is financed through a regulated financial business, the Supervised Firm must seek to establish the underlying origin of the funds.

The nature and extent of the information and documentation required to establish SoF will depend on the circumstances of the transaction and the information provided by the client. The SoF documentation process should focus on where the funds originated, how they were accumulated by the client and whether there is any indication that they may represent the proceeds of crime.

Depending on the circumstances, useful evidence may include:

- bank statements;
- payslips or employment records;
- audited financial statements;
- sale and purchase agreements;
- probate documents or wills;
- loan agreements; or
- receipts or completion statements from prior transactions.

Where it is known that a third party is contributing to the funds, the Supervised Firm should consider whether it is necessary to establish the third party's own SoF, informed by the level of risk.

The extent of third-party SoF enquiries should take into account that the acceptance of funds from unknown or unconnected third parties is a specific risk factor under the AMLRs. The depth of SoF enquiries must be informed by the ongoing assessment of client/matter risk and must be capable of being justified by reference to the BRA and sectoral risk assessments.

Where funds have become mixed with other monies, it may not be possible to establish SoF without some understanding of the client's underlying SoW. In such cases, the Supervised Firm may need to consider SoW as part of its assessment.

6.7.2 Source of Wealth

SoW refers to the origin of a client's overall wealth or net worth. It describes the economic, business or commercial activities that generated, or significantly contributed to the client's entire body of assets. The purpose of establishing SoW is to understand why and how the client has accumulated their overall level of wealth, rather than to explain any specific transaction in isolation.

Supervised Firms' assessment of SoW should recognise that wealth-generating activities may change over time as new activities are undertaken and further wealth is accumulated.

In lower or medium risk cases, it may be sufficient to establish SoW by:

- obtaining and recording the client's explanation of how their wealth was accumulated; and
- corroborating this, where appropriate, through public sources or basic verification of business interests.

In relation to corporate clients, the Supervised Firm may be satisfied where the transaction appears consistent with what is known about the entity's business activities and financial profile. For higher-risk situations, more detailed enquiries and independent verification of SoW will be required, as set out in the EDD section.

6.8 Enhanced Due Diligence (EDD)

6.8.1 Purpose of EDD

EDD can assist in strengthening the Supervised Firm's knowledge of the client/applicant and any beneficial owner(s) and whether the instruction and any transaction(s) are consistent with what the Supervised Firm knows about the client, the client's background and their financial circumstances.

In accordance with regulation 27, EDD must be applied where:

- a higher ML/TF/PF risk has been identified under the Supervised Firm's risk assessment framework;
- supervisory guidance identifies a high risk of ML/TF/PF;
- the client/applicant is from a foreign country identified by credible sources as having serious deficiencies in its AML/CFT/CPF regime or a prevalence of corruption;
- the relationship involves correspondent banking (pursuant to Part 11 of the Regulations, where applicable);
- the client/applicant is a PEP;
- there is unusual or suspicious activity; or
- the business relationship or transaction is with a person from a country for which FATF has requested enhanced measures.

EDD should be proportionate to the risk and should focus on answering, with appropriate evidence:

- Why the client is seeking the service/relationship and whether it makes sense;
- What the transaction/activity is intended to achieve, and whether the stated purpose is credible;
- How the transaction will operate in practice (who, what, where, and why); and
- Whether the activity could indicate ML/TF/PF concerns.

6.8.2 Examples of EDD Measures

EDD is not limited to a prescribed checklist. Measures should be selected and scaled to address the risk driver(s). Depending on circumstances, EDD measures may include the following:

Deepen the Client Profile

- obtain additional information on the client (occupation, business interests, asset profile, residency and jurisdictional links);
- obtain additional information on beneficial owners/controllers (including identifying additional individuals where the structure warrants it); and
- corroborate key statements through independent and reliable sources (registries, reputable databases, professional references, open sources).

Strengthen the Understanding of the Relationship/Instruction

- obtain additional information on the intended nature and purpose of the relationship;

- obtain and test the rationale for the structure (including why particular entities/jurisdictions/intermediaries are involved); and
- obtain further information on counterparties where material to the risk/conducting checks on counterparties.

Receive Financial Context

- obtain additional information and evidence on SoFs for the matter/transaction;
- obtain additional information and evidence on SoW where relevant (and in particular for PEPs—see Section 6.7); and
- obtain information on the reasons for the transaction(s), including documentary support where appropriate.

Governance and Approvals

- require senior management approval to commence or continue a relationship where the risk warrants it (and where required for PEPs).

6.8.3 Complex, unusual or unexplained transactions

Supervised Firms should examine, as far as reasonably possible, the background and purpose of complex transactions, unusually large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose. Supervised Firms should also use EDD measures where appropriate to resolve concerns or to determine whether the activity is suspicious.

Where concerns cannot be resolved, the Supervised Firm should consider whether suspicion has arisen and whether reporting is required and must manage tipping-off risk where relevant.

6.8.4 High-risk Jurisdictions

Certain jurisdictions may present increased risk due to corruption, organised crime, weak AML/CFT/CPF regimes, sanctions exposure, or FATF status. Under regulation 8A, firms must take account of credible sources and must not treat a jurisdiction as low risk where specified red-flag criteria are present. Please refer to Chapter 5 for more information on high-risk jurisdictions.

Where a client, beneficial owner, counterparty, or key transactional element is connected to such a jurisdiction, Supervised Firms should apply EDD targeted to the specific risk. This may include:

- more robust corroboration of identity and control;
- enhanced SoF/SoW enquiries;
- careful scrutiny of the commercial rationale and transaction background; and
- heightened caution around acceptance of certified documents from high-risk jurisdictions (including verifying the certifier's legitimacy, where appropriate).

6.9 Politically Exposed Persons (PEPs)

Business relationships involving PEPs can expose the Supervised Firm to heightened ML/TF/PF risk, particularly corruption and bribery risk, due to the client's access to public funds, influence, and potential conflicts of interest. PEP status does not automatically require refusal of instructions, but it does require specific mandatory controls under the AMLRs.

6.9.1 Categories of PEPs

Individuals identified as PEPs may fall within the following categories:

- Foreign PEPs: individuals entrusted with prominent public functions by a foreign country, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials;
- Domestic PEPs: individuals entrusted domestically with prominent public functions, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials; and
- International organisation PEPs: individuals entrusted with prominent functions by an international organisation, including members of senior management, such as directors, deputy directors, board members, or persons performing equivalent functions.

For the purposes of the AMLRs, PEP requirements also apply to family members and close associates of PEPs.

- (a) Family members include a spouse, civil partner, parent, sibling, or child of a PEP.
- (b) Close associates include any natural person who is known to:
 - i. have joint beneficial ownership of a legal person or legal arrangement with a PEP;
 - ii. maintain a close business or personal relationship with a PEP; or
 - iii. have beneficial ownership or control of a legal person or legal arrangement that is known to have been established for the benefit of a PEP.

6.9.2 Mandatory requirements when dealing with PEPs

Where the Supervised Firm has a business relationship with a PEP (or a family member/close associate), the AMLRs require Supervised Firms to implement risk management systems and procedures that:

1. Determine whether a client or beneficial owner of that client is a PEP, family member or close associate;
2. Require senior management approval before establishing or continuing a business relationship with a PEP (or family member/close associate);
3. Take reasonable measures to establish the SoW and SoF of the person involved in the business relationship and of the beneficial owner identified as a PEP (or family member/close associate); and
4. Monitor PEP business relationships as a component of the Supervised Firm's procedures.

6.9.3 PEP Identification in Practice (Systems and Controls)

PEP identification should be embedded into onboarding and, where relevant, refresh events. Proportionate methods may include:

- client/representative declarations (PEP questions within the onboarding form);
- screening using reputable electronic tools or databases (particularly where the client base makes PEP exposure more likely);
- targeted open-source checks where tool-based screening is not used, or where results are unclear; and
- escalation triggers where staff become aware of information suggesting PEP exposure (e.g., public office, government correspondence, state-linked funding).

Where results are uncertain, the file should record the steps taken to resolve uncertainty and the basis for the Supervised Firm's conclusion (including if it proceeds on the basis of applying enhanced measures).

6.9.4 Change in PEP Status

Where a client or beneficial owner is identified as a PEP after onboarding, the Supervised Firm must apply the same controls, including senior management approval to continue and taking reasonable measures to establish SoW/SoF.

Where a person is no longer in office, the Supervised Firm should adopt a proportionate approach to whether to continue to treat them as a PEP, having regard to continuing influence, continuing networks, and whether their prior role remains relevant to the risks presented.

6.10 **Simplified Due Diligence (SDD)**

SDD is not the absence of due diligence; it is a calibrated approach in which the firm may apply simplified measures that are commensurate with the low-risk factors identified.

When determining whether SDD is appropriate, the Supervised Firm must ensure that the assessment of risk is consistent with the NRA and must pay particular attention to the risk level assigned to the relevant sector, client type, and activity. Where the Supervised Firm applies SDD, the rationale must be clearly documented and made available to the LSSA on request.

6.10.1 The Application of SDD

SDD may be applied only where all of the following conditions are met:

- the Supervised Firm has assessed the relationship/transaction as presenting a low level of ML/TF/PF risk and the finding is consistent with the NRA or the Supervisory Authority, whichever is most recently issued;
- the Supervised Firm knows the identity of the applicant/client and (where relevant) has identified the beneficial owner(s);
- the Supervised Firm knows the nature and intended purpose of the business relationship or one-off transaction;

- there is no knowledge, suspicion, or reasonable grounds to suspect ML/TF/PF (including where the applicant/ client is acting on behalf of another person engaged in ML/TF); and
- must be an acceptable applicant as set at 6.10.4 below.

6.10.2 Cases where SDD is Prohibited

SDD must not be applied where:

- the Supervised Firm has identified the client as being of a higher-risk;
- the Supervised Firm knows, suspects, or has reasonable grounds for knowing or suspecting ML/TF/PF or other forms of criminal conduct;
- the circumstances suggest the client is acting on behalf of a person engaged in ML/TF/PF; or
- the client type or matter is identified as higher-risk in the NRA or supervisory guidance.

In these circumstances, the Supervised Firm must revert to standard CDD or apply EDD as appropriate, and follow the firm's documented escalation and reporting processes where suspicion arises.

6.10.3 Examples of SDD measures

Where SDD is appropriate, the Supervised Firm may consider applying simplified measures such as:

- reducing the frequency of client identity refresh and update cycles; and/or
- relying on a third party for the verification of identity (subject to the reliance requirements and restrictions in the AMLRs and these Guidance Notes).

Where the Supervised Firm uses digital ID systems or e-KYC processes, lower levels of assurance may be acceptable only in low-risk cases, provided the Supervised Firm has documented controls to ensure the method remains reliable and appropriate for the circumstances.

6.10.4 Other Acceptable Applicants

The AMLRs permit the Supervised Firms, in defined cases and subject to the conditions above, to defer or simplify verification for certain types of clients. These include:

- persons conducting RFB and otherwise subject to the AMLRs (or majority-owned subsidiaries of such businesses);
- central or local government organisations, statutory bodies, or agencies of government in countries assessed as having a low ML/TF/PF risk;
- regulated overseas entities (or majority-owned subsidiaries) where the overseas regulator exercises AML/CFT/CPF supervision and the entity is formed/incorporated/based in a low-risk country;
- companies listed on a recognised stock exchange and subject to disclosure requirements that provide transparency of beneficial ownership (and majority-owned subsidiaries); and
- certain pension fund arrangements as described in the AMLRs.

The Supervised Firm should apply SDD only where the applicant clearly falls within an eligible category and the Supervised Firm's risk assessment supports a low-risk outcome. In accordance with regulation 22(2), Supervised Firms must document its basis for determination for applying SDD to the clients. This should be readily available upon request by the LSSA.

6.11 Reliance on Third Parties

Supervised Firms are required under the AMLRs to maintain identification procedures that result in the production of satisfactory evidence of identity of clients. According to the AMLRs, evidence of identity is satisfactory if it is reasonably capable of establishing that the applicant is the person he claims to be and the person who obtains the evidence is satisfied, in accordance with the procedures maintained under these regulations in relation to the Supervised Firm concerned, that it does establish that fact.

Where the risks are low and where there is no knowledge, suspicion or reasonable grounds of ML/TF/PF, subject to the conditions outlined in regulation 22, Supervised Firms may rely on third parties for verification of identification of clients and beneficial owners.

However, reliance on a third party does not remove or diminish the Supervised Firm's responsibility for compliance with its CDD obligations under the AMLRs.

6.11.1 Nominees or Agents Acting for a Principal

Where a client appears to act as a nominee or agent for a principal, a Supervised Firm may rely on the nominee or agent to carry out verification of the principal only where the nominee or agent itself qualifies as an acceptable applicant for the purposes of SDD.

A Supervised Firm must not rely on such a nominee or agent unless the nominee or agent provides written assurance confirming that it has:

- identified and verified the principal (and beneficial owner(s), where applicable);
- established the nature and intended purpose of the relationship/transaction;
- identified the SoF of the principal; and
- undertaken to provide identification/verification data and relevant documents without delay on request.

Where reliance is placed on such written assurance, the Supervised Firm remains fully accountable for any failure by the third party to perform its CDD obligations adequately, including any failure to obtain, retain, or provide the required CDD information or documentation.

6.11.2 Introduced Business (Eligible Introducers)

Where a client is introduced by an eligible introducer, a Supervised Firm should rely on the introducer's CDD procedures only where the introducer:

- meets the eligibility criteria of an acceptable applicant under the AMLRs (see regulation 22(1)(d)); and
- provides written assurance confirming:
 - the identity of the client, and where applicable, the beneficial owner;

- the nature and intended purpose of the business relationship;
- that the introducer has identified and verified the identity of the client (and any beneficial owner) in accordance with procedures maintained under applicable laws;
- that the introducer has identified the SoF of the client;
- that the introducer is supervised or monitored by a SA or overseas regulatory authority and has appropriate measures in place to ensure compliance with CDD and record keeping requirements; and
- that the introducer shall make available on request and without delay, copies of identification and verification data and any other relevant documentation relating to the CDD requirements in respect of the client (and beneficial owner, where applicable).

Reliance on an eligible introducer should be approved by senior management. The decision to rely on the introducer must be documented, including the reasons why it was reasonable not to apply normal verification measures directly and why reliance is appropriate in the circumstances.

Reliance must not be used where the Supervised Firm:

- knows or suspects ML/TF involving the introducer, applicant, or any relevant third party;
- has reason to doubt the identity of the applicant, introducer, or beneficial owner; or
- is not satisfied that the CDD data and documents will be made available without delay.

Supervised Firms that rely on eligible introducers should periodically test the introducer's ability to produce CDD documentation promptly, record the results of those tests, and document remedial action where issues are identified. Notwithstanding any reliance arrangements, Supervised Firms remain legally responsible for compliance with the AMLRs and are liable for any failure by an introducer to obtain, maintain, or provide satisfactory CDD information and documentation when required.

CHAPTER 7 – ONGOING MONITORING

7.1 Statutory Obligations and Scope

Regulation 12(1)(e) of the AMLRs requires Supervised Firms to conduct ongoing monitoring of business relationships. Ongoing monitoring includes:

- scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the SoF), to ensure that those transactions are consistent with the Supervised Firm's knowledge of the client, the client's business and the assessed risk profile; and
- reviewing existing records to ensure that documents, data and information obtained for CDD purposes remain current, accurate and adequate.

In the legal sector, this obligation must be applied in a proportionate and risk-based manner, recognising that some legal engagements involve single matters rather than long-term, account-based relationships. Ongoing monitoring in a legal practice does not require continuous transactional surveillance of the kind expected of financial institutions. However, it does require Supervised Firms to remain alert to changes, inconsistencies or developments that may affect their understanding of the client, or risks associated with the instructions.

Accordingly, ongoing monitoring in a legal context may occur:

- during the lifecycle of a single matter, particularly where the matter spans over time, involves multiple stages, or includes the movement of client funds; and
- when new instructions are received from an existing client, even where no continuous relationship is otherwise maintained.

Supervised Firms should therefore consider whether the CDD information already held remains appropriate for the instructions being undertaken, rather than assuming that CDD completed at the outset of a prior matter remains sufficient in all cases.

This section does not replace or restate the Supervised Firm's substantive obligations relating to identification, verification, beneficial ownership, SoF or SoW, or EDD, which are addressed elsewhere in these Guidance Notes. It explains how and when those measures may need to be revisited as part of ongoing monitoring.

7.2 Scrutiny of Transactions

Regulation 12(1)(e) requires Supervised Firms to scrutinise transactions to ensure that they are consistent with the Supervised Firm's knowledge of the client, the purpose and intended nature of the relationship, and the assessed risk profile.

In the legal sector, transactional scrutiny will typically focus on:

- whether funds received are consistent with the stated purpose of the matter;
- whether the SoF matches what was previously disclosed or expected; and
- whether funds are received from unexpected third parties or jurisdictions.

This does not require a re-performance of SoF or SoW checks each time funds are received. Rather, Supervised Firms should remain alert to developments during a matter that may indicate that further enquiries are required, particularly where funds are received in stages, funding arrangements change, or additional contributors become involved.

Ongoing monitoring may be triggered by events or information that suggest a change in risk or a need to reassess the adequacy of existing CDD. Such triggers may include, for example:

- changes in client identity information (e.g. name, address or nationality);
- changes in beneficial ownership or control;
- new involvement of higher-risk jurisdictions;
- unexpected changes in the nature or purpose of the instructions; or
- information suggesting sanctions exposure, PEP status or adverse media.

Where such issues arise, Supervised Firms must make appropriate enquiries, assess the risk implications, and document the outcome. Where concerns cannot be satisfactorily resolved, Supervised Firms should consider whether suspicion has arisen and whether reporting obligations are engaged, taking care at all times to manage the risk of tipping-off.

7.3 Refreshing and Reapplying CDD Measures

In accordance with regulation 17A of the AMLRs, Supervised Firms must apply CDD measures to existing clients on a risk-based basis at appropriate times. Supervised Firms may rely on identification and verification previously obtained, unless there is uncertainty whether CDD remains current and sufficient. This obligation also does not require periodic re-verification on a fixed or arbitrary schedule. Instead, Supervised Firms must consider whether CDD information remains adequate and up to date, having regard to:

- when CDD was last completed;
- the level of ML/TF/PF risk associated with the client or matter; and
- any changes in the client's circumstances, ownership, control or the nature of the instructions.

Ongoing monitoring under regulation 12(1)(e) should inform decisions as to when CDD must be refreshed or reapplied under regulation 17A.

In a legal practice, this may include circumstances where:

- a client provides new or materially different instructions from those previously undertaken;
- there has been a significant gap between engagements, particularly in higher-risk matters;
- the structure, counterparties or jurisdictions involved in a matter change; or
- information obtained during the matter suggests that earlier CDD may no longer be reliable.

Refreshing CDD does not automatically require full re-verification in every case. However, Supervised Firms must be able to demonstrate why reliance on existing CDD remains reasonable, or why additional steps were taken. As a general guide (and not a fixed rule), a lapse of twelve months or more between matters may warrant closer review in higher-risk situations, taking account of the Supervised Firm's client, matter and business risk assessments.

7.4 Evidence of Monitoring

Supervised Firms must be able to demonstrate compliance with their ongoing monitoring obligations under regulation 12(1)(e).

Each instance of ongoing monitoring, whether during a matter or when new instructions are received, should be appropriately documented. Records should, where relevant, capture:

- what information or activity was reviewed;
- whether any issues or inconsistencies were identified;
- what action was taken, or why no action was considered necessary;
- the rationale for the decision reached; and
- who undertook the review and when.

Such records may take the form of file notes, updated risk assessments or internal review logs and must be retained in accordance with the Supervised Firm's record-keeping obligations under the AMLRs.

CHAPTER 8 – RECORD KEEPING PROCEDURES

8.1 Obligations Under the AMLRs

Effective record keeping is fundamental to a Supervised Firm's ability to demonstrate compliance with the AML/CFT/CPF regime and the proper application of an RBA. Accurate, complete and retrievable records support supervisory oversight, facilitate cooperation with CAs and law enforcement, and provide evidential protection to the Supervised Firm, its principals and staff where decisions are subsequently scrutinised.

Across all aspects of AML/CFT/CPF compliance, Supervised Firms are expected to document the rationale for decisions involving the exercise of judgement, particularly where those decisions are informed by the RBA. Records created at the time the decision is taken will generally carry greater evidential weight than explanations produced retrospectively.

In accordance with Part 8 of the AMLRs, Supervised Firms must establish and maintain record-keeping procedures as part of their AML/CFT/CPF policies and procedures. The procedures should clearly set out:

- (i) the categories of AML/CFT/CPF records retained;
- (ii) where and how records are stored, including whether records are held electronically or centrally;
- (iii) responsibilities for creation, review, approval and filing of records;
- (iv) applicable retention periods and protocols for secure destruction;
- (v) controls governing confidentiality, access and integrity of records; and
- (vi) procedures for responding promptly to requests from CAs.

Supervised Firms are required to retain records relating to CDD, transactions and business relationships that are sufficient to permit the reconstruction of individual transactions and to support investigations and prosecutions of ML/TF/PF offences.

Supervised Firms must retain, at a minimum, records of identification and verification data obtained through the CDD process beneficial ownership information, account files and business correspondence, records of transactions carried out (together with supporting documentation) and records of analyses undertaken in relation to unusual or suspicious activity.

Such records must be retained for a minimum of five years from the date on which the business relationship ends or, in the case of a one-off transaction, from the date on which that transaction is completed. A one-off transaction is deemed to be completed when all activities undertaken in the course of that transaction have been concluded, including where the firm knows, suspects, or has reasonable grounds to suspect ML/TF/PF.

Where a SAR has been submitted, or where the Supervised Firm is aware of an ongoing investigation relating to ML/TF/PF involving a client or transaction, all records relating to that client or transaction must be retained until confirmation is received that the matter has been fully concluded.

Records must be maintained in a manner that enables their prompt retrieval and production without delay upon request by the LSSA, the FRA, or any other SA or CA. Any record that cannot be located or produced without delay may be treated by SAs as if it does not exist.

Records may be retained in original form, as copies, or in electronic format, provided that they are complete, accurate, and capable of being relied upon for evidential purposes. Supervised Firms must ensure the integrity

of records throughout the retention period, including protection against unauthorised alteration or deletion, and must implement appropriate controls to ensure authenticity, traceability, and reliability. The format in which records are retained must not impede the Supervised Firm's ability to comply promptly with lawful requests from CAs.

8.2 Scope of Records to Be Retained

8.2.1 Client Due Diligence Records

Supervised Firms must retain records evidencing compliance with CDD requirements. These records should comprise a description of the nature of the identification and verification evidence obtained, together with the evidence itself, a copy of it, or information reasonably sufficient to obtain such a copy.

Beneficial ownership information forms part of the CDD record set and must be retained for at least five years after the date on which the client ceases to be a client or, after the date on which a client which is a legal entity is dissolved or otherwise ceases to exist.

8.2.2 Transaction Records

Records relating to transactions must be sufficient to enable individual transactions to be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity. Depending on the nature of the Supervised Firm's activities, this may include details of the client, beneficial owner and any counterparty, the nature and purpose of the transaction, relevant dates, values and currencies, the form in which funds are offered and paid, sources and destinations of funds or bearer securities, memoranda of instructions and authorities, book entries and account movements, and custody or title documentation where applicable.

Records should also include documentation and analysis relating to complex or unusually large transactions, unusual patterns of transactions, or transactions lacking apparent economic or legal purpose, together with the conclusions reached.

8.2.3 Risk Assessment Records

In applying an RBA, Supervised Firms must retain records evidencing their BRA, client or matter-specific risk assessments, and the rationale for key AML/CFT/CPF decisions. This includes records explaining the level of CDD applied, decisions to apply simplified or enhanced measures, the frequency and scope of ongoing monitoring, and conclusions reached following the review of unusual or complex transactions. These records form part of the AML/CFT/CPF records required to be retained under Part 8 of the AMLRs.

8.2.4 Training Records

To demonstrate compliance with AML/CFT/CPF training obligations, Supervised Firms should retain training records. Further details can be found at Chapter 9 below.

8.3 Group Records

Where records are maintained centrally or outside the Cayman Islands, including within a group structure, Supervised Firms must ensure that records are maintained in accordance with the AMLRs and can be retrieved and provided promptly and without delay to the SA and other CAs.

8.4 Registers of Enquiries and Disclosures

Supervised Firms should maintain a separate register of all enquiries received from the FRA and Law Enforcement Agencies (LEAs) and all disclosures made to the FRA and LEAs. This register should be kept separate from other records and should include, at a minimum, the date and nature of each enquiry or disclosure and details of the relevant client, account or matter. The register should be retained for at least five years after the termination of the relevant business relationship.

8.5 Reliance and Delegation

Where a Supervised Firm delegates functions or relies on third parties for the performance of AML/CFT/CPF measures, the Supervised Firm remains responsible for compliance with the AMLRs and must be satisfied that records relating to those functions are maintained in accordance with regulatory requirements. Supervised Firms should document the basis on which accessibility and equivalence of record-keeping arrangements have been assessed. The Supervised Firm should also retain evidence that third-party arrangements are subject to adequate oversight, periodic reviews and testing of the effectiveness of third-party AML/CFT/CPF and sanctions controls and any steps taken to resolve identified deficiencies. Records must be made available to the LSSA or other CAs upon request.

8.6 Data Protection and Confidentiality

In maintaining AML/CFT/CPF records, Supervised Firms must comply with the DPA while also observing professional duties of confidentiality and, where applicable, LPP. Personal data contained in CDD records, transaction and matter files, risk assessments and internal reports must be processed fairly and lawfully, used only for specified and legitimate purposes, and retained no longer than is necessary, subject always to the statutory record-keeping obligations imposed by the AMLRs and other applicable laws. The lawful basis for such processing will ordinarily include compliance with a legal obligation and the prevention or detection of crime.

Supervised Firms should implement appropriate technical and organisational measures to protect AML/CFT/CPF records against unauthorised access, loss, alteration or disclosure. This includes restricting access to AML/CFT/CPF records on a strict need-to-know basis, segregating AML/CFT/CPF records (including internal reports and SAR-related material) from client-facing matter files where appropriate and ensuring that both physical and electronic records are stored securely. Particular care should be taken to prevent inadvertent disclosure of sensitive AML/CFT/CPF information to clients or third parties, including in circumstances that could give rise to tipping-off or prejudicing an investigation.

The DPA does not prevent the retention, use or disclosure of personal data where such processing is required for compliance with AML/CFT/CPF obligations, for responding to lawful requests from CAs, or for the prevention or detection of crime. Statutory AML/CFT/CPF record-keeping requirements constitute a lawful justification for the retention of personal data for the applicable retention period. Where the exercise of data subject rights, including rights of access or erasure, would be likely to prejudice AML/CFT/CPF obligations, regulatory or supervisory functions, or the prevention or detection of crime, Supervised Firms may rely on the applicable exemptions under the DPA. Supervised Firms should document the basis on which such exemptions are applied and ensure that AML/CFT/CPF records are securely destroyed or deleted once the applicable retention period has expired and no lawful basis for continued retention exists.

CHAPTER 9 – TRAINING

9.1 Importance of Training

Partners, employees and agents who provide services to clients represent the Supervised Firm's first and most effective line of defence against the risk of becoming inadvertently involved in ML/TF/PF. Effective AML/CFT/CPF training is therefore a core component of a Supervised Firm's systems, policies, procedures and controls, and a critical measure for mitigating ML/TF/PF risks.

Training should provide relevant individuals with sufficient awareness, skills and knowledge to understand the Supervised Firm's AML/CFT/CPF obligations under Cayman Islands law, to recognise risk indicators relevant to their role, to apply internal policies and procedures correctly and consistently, and to escalate concerns promptly and appropriately through established internal reporting channels.

Training should not be treated as a one-off or purely formal exercise. It should support the effective operation of the Supervised Firm's RBA and reinforce a culture of compliance, accountability and professional judgement across the organisation.

9.2 Regulatory Requirement

Under regulation 5(c) and (d) of the AMLRs, Supervised Firms are required to take appropriate measures to ensure that their employees are made aware of the AML/CFT/CPF laws, regulations and obligations applicable to their role; and provided ongoing training in the recognition and handling of transactions or activities that may be related to ML/TF/PF, including assets subject to TFS.

What constitutes "appropriate measures" will depend on the nature, size and complexity of the Supervised Firm and the ML/TF/PF risks identified through the BRA. A proportionate RBA must therefore be applied to the design, delivery and frequency of training.

9.3 Training Programme

9.3.1 Scope

Supervised Firms should document their approach to AML/CFT/CPF training within their written policies and procedures. The training framework should be approved by senior management and reviewed periodically to ensure it remains appropriate and effective.

As part of this framework, Supervised Firms should consider and document:

- how the effectiveness of training is assessed, including whether training outcomes are reflected in day-to-day conduct and decision-making;
- the frequency of training and the circumstances that trigger refresher or enhanced training;
- how training content is tailored to different roles, responsibilities and levels of risk exposure; and
- how training completion and competence are recorded, monitored and escalated where gaps are identified.

Where there are material changes to legislation, supervisory guidance, the Supervised Firm's risk profile or its internal policies and procedures, training programmes should be updated promptly, communicated clearly and where necessary training provided to relevant persons.

9.3.2 Who Should Receive Training

AML/CFT/CPF training must be provided to all staff of a Supervised Firm, regardless of role, as an integral element of establishing and maintaining an effective compliance culture. Every member of staff should receive general AML/CFT/CPF training sufficient to ensure an appropriate level of awareness of the Supervised Firm's obligations under the AMLRs, the risks of ML/TF/PF, and the importance of compliance with internal policies and procedures.

In addition to general training, Supervised Firms are required to provide enhanced or role-specific training to individuals whose functions expose them to higher ML/TF/PF risk or who are directly involved in the operation of the AML/CFT/CPF framework. This includes individuals who, by virtue of their role, are capable of contributing to compliance with the AMLRs, the identification, mitigation or management of ML/TF/PF risks, or the prevention, detection or escalation of suspicious activity.

Depending on the structure and activities of the Supervised Firm, this may include fee earners, compliance and risk personnel, finance and accounts staff, and support staff who interact with clients, handle client funds or documentation, or assist with client onboarding, ongoing monitoring or record-keeping.

Training should be proportionate to the individual's role, responsibilities and level of exposure to ML/TF/PF risk. However, no member of staff should be excluded entirely from AML/CFT/CPF training. Supervised Firms should be able to demonstrate that general training is consistently delivered across the organisation, and that additional, targeted training is provided where required by risk.

9.3.3 Content of Training

AML/CFT/CPF training should be tailored to the Supervised Firm's activities, services and risk profile and should enable relevant persons to identify and respond appropriately to risk indicators encountered in practice.

As a minimum, training should cover:

- the AML/CFT/CPF legal and regulatory framework applicable in the Cayman Islands;
- the Supervised Firm's BRA and key risk factors;
- internal policies and procedures, including CDD, EDD, ongoing monitoring and sanctions screening;
- recognition of suspicious activity and the firm's internal reporting procedures;
- obligations relating to tipping off, confidentiality and LPP; and
- record-keeping and data protection requirements.

Training should be role-specific where appropriate, with enhanced or specialised training provided to individuals involved in higher-risk work, complex transactions or decision-making under the RBA.

9.3.4 Delivery Methods

Training may be delivered through a variety of methods, including internal or external training sessions, online modules, webinars, attendance at relevant conferences or workshops, review of internal materials, and completion of recognised AML/CFT/CPF qualifications.

Supervised Firms should not rely solely on attendance as evidence of effective training. Consideration should be given to how learning outcomes are assessed, for example through testing, practical case studies, feedback, file reviews or supervisory oversight, and how deficiencies are identified and addressed.

9.3.5 Frequency and Timing

New employees and agents should receive AML/CFT/CPF training as soon as practicable after joining the Supervised Firm and, where possible, before undertaking any regulated or client-facing activities.

Refresher training should be provided at regular and appropriate intervals. As a minimum, Supervised Firms should consider providing AML/CFT/CPF awareness training to all staff on an annual basis, supplemented by additional role-specific or enhanced training where this is justified by the firm's risk profile or by an individual's responsibilities.

Additional or ad hoc training should be provided where there are material changes to AML/CFT/CPF legislation or supervisory guidance, changes to the Supervised Firm's policies, procedures or controls, changes to an individual's role or responsibilities, or the emergence of new or evolving risks, typologies or red flags relevant to the Supervised Firm's activities.

9.4 Training for Sole Practitioners and Small Firms

Where a Supervised Firm operates as a sole practitioner or a very small firm, the practitioner should ensure that they personally receive adequate AML/CFT/CPF training to protect the practice from ML/TF/PF risks. This includes maintaining up-to-date knowledge of legislative requirements, risk indicators relevant to the practice area, and internal reporting and compliance obligations.

Sole practitioners and small firms should retain records of all AML/CFT/CPF training undertaken and should periodically assess whether additional or specialist training is required in light of changes to their services, client base or risk profile.

9.5 Specific training for AMLCOs, MLROs and DMLROs

AMLCOs, MLROs and DMLROs should receive enhanced and in-depth training commensurate with the seniority, responsibilities and decision-making authority of their roles.

Supervised Firms should consider whether specialist or advanced training is required to ensure that individuals appointed to these roles are competent to discharge their functions effectively. Such training should support a sound understanding of the interpretation and application of primary AML/CFT/CPF legislation, the assessment and investigation of suspicious activity, decision-making and reporting obligations, and effective interaction with the LSSA and CAs. Training should also address emerging risks, typologies and enforcement trends relevant to the Supervised Firm's activities.

AMLCOs, MLROs and DMLROs should keep themselves informed of relevant supervisory guidance, thematic reviews and enforcement outcomes published by the LSSA and other CAs, as part of maintaining their ongoing competence and effectiveness in role.

9.6 Training Records

Supervised Firms should maintain comprehensive and accurate records of AML/CFT/CPF training, including:

- training materials and content;
- names and roles of individuals trained;
- completion records;
- dates of training; and
- results of any assessments or evaluations.

Training records, which include ongoing training plans, should be retained in accordance with the Supervised Firm's record-keeping obligations and must be made available to the LSSA upon request.

CHAPTER 10 – SUSPICIOUS ACTIVITY REPORTING

10.1 Introduction

The FATF Standards require jurisdictions to establish effective suspicious transaction reporting systems applicable to legal professionals when they engage in RFB activity.^{16 17} Pursuant to POCA, the FRA is responsible for receiving, requesting, analysing and disseminating disclosures of information concerning the proceeds of criminal conduct, suspected proceeds of criminal conduct or other information required under relevant legislation to counter ML/TF/PF.

Suspicious activity reporting is an essential component of the Cayman Islands' AML/CFT/CPF framework. Disclosures made by legal professionals and other persons within the supervised sector provide valuable intelligence to competent authorities and support the prevention, detection and disruption of financial crime.

Further information regarding the FRA and its functions is available at: www.fra.gov.ky.

Suspicious activity reporting should not be used as a substitute for adequate CDD or effective internal controls. Rather, it is intended to ensure that knowledge or suspicion (or reasonable grounds for knowledge or suspicion) of ML, TF or PF is promptly escalated, assessed by the MLRO and disclosed to the FRA.

10.2 Application

The reporting obligations under POCA apply to all natural and legal persons in, or undertaking activities within the Cayman Islands, including legal professionals carrying out RFB. Where reporting obligations arise, disclosures must be made to the FRA subject to legal professional privilege.

In practice, reporting obligations may arise in several circumstances, including where a person:

- knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in criminal conduct;
- knows or suspects or has reasonable grounds for knowing or suspecting, that property is criminal property, i.e. it constitutes or represents a person's benefit from criminal conduct which includes terrorist property; or
- becomes aware of information indicating that a transaction or attempted transaction may be connected to ML, TF, PF or other criminal conduct.

In addition to obligations placed on persons, the TA also imposes disclosure obligations in relation to suspected terrorist property.

¹⁶ Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (updated 16 October 2025).

¹⁷ FATF, Guidance for a Risk-Based Approach for Legal Professionals (2019).

10.3 Internal Reporting Procedures

Under Part 9 of the AMLRs, Supervised Firms are required to maintain internal reporting procedures designed to ensure that knowledge or suspicion or reasonable grounds for knowing or suspecting ML, TF or PF is appropriately escalated and assessed.

These internal procedures are distinct from, but designed to facilitate compliance with, the statutory obligation to make external disclosures to the FRA under POCA and the TA.

Internal reporting procedures must identify the MLRO and specify that the MLRO is the person to whom a report must be made where information or other matters come to the attention of a person carrying out relevant financial business which, in that person's opinion, give rise to knowledge or suspicion, or reasonable grounds for knowing or suspecting, that another person is engaged in criminal conduct, or that a transaction or attempted transaction relates to criminal conduct.

Please note that the TA has specific triggers, for example knowledge or suspicion of terrorist property or property being used for terrorism.

Internal reporting procedures should also require that any internal report is considered by the MLRO or DMLRO in light of all other relevant information available within the firm for the purpose of determining whether the information gives rise to such knowledge or suspicion. The MLRO or DMLRO must have access to any information within the firm that may assist in carrying out this assessment.

Where, after considering the report and all relevant information, the MLRO knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in criminal conduct, the matter must be disclosed to the FRA.

Internal reporting procedures should also provide practical guidance on how internal reports are to be made in practice. This may include specifying the reporting channel to be used, the information that should be included in a report, and arrangements for handling confidential information to minimise the risk of tipping off.

10.4 Role of the MLRO

The MLRO serves as the central point within a firm for receiving and assessing internal disclosures relating to potential criminal conduct.

Upon receipt of an internal report, the MLRO (or DMLRO) should assess the information in light of all other relevant information available to the firm, including:

- client due diligence information;
- details of the relevant matter or transaction; and
- any other information held by the firm relating to the client or transaction.

Where appropriate, the MLRO may undertake limited internal enquiries to clarify the circumstances of the report. However, any such enquiries must be carefully controlled to avoid tipping off a client or prejudicing a potential investigation.

If the MLRO determines that the statutory reporting threshold has been met and that disclosure is permissible (having regard to legal professional privilege), the MLRO must ensure that a disclosure is made promptly to the FRA.

Where the MLRO determines that a disclosure is not required, the reasons for that decision should be documented and retained with the internal report.

10.5 Suspicious Activity Reports

10.5.1 What is a SAR?

A SAR is the disclosure made to the FRA under POCA.

From a risk-based perspective, legal professionals should ensure that SAR decision-making and narrative drafting is supported by:

An understanding of the client, beneficial owner(s) and purpose/intended nature of the relationship/transaction;

Appropriate scrutiny of complex or unusually large transactions with no apparent lawful purpose; and

Prompt internal escalation to the MLRO/DMLRO where suspicion arises.¹⁸

10.5.2 Who Makes the disclosure?

Where a firm has appointed a MLRO, the MLRO (or DMLRO in their absence) will generally be responsible for making external disclosures to the FRA following receipt and assessment of an internal report.

10.5.3 When should a SAR be filed?

A SAR must be filed as soon as practicable after a suspicion of criminal conduct has been formed.

Suspicion may arise from a single event or transaction or an accumulation of factors or information.

Legal professionals should escalate concerns internally even where they are uncertain whether the reporting threshold has been met, so that the MLRO can assess the matter using all relevant information available to the firm.

10.5.4 How to Submit a SAR

The FRA has established mechanisms for the filing of SARs. Reporting entities can register with the FRA to file using the AMLive electronic portal. Alternatively, SARs may be submitted by secure email, using the prescribed SAR form, to FinancialReportingAuthority@gov.ky.

Further information on filing procedures is available on the FRA's website.

¹⁸ FATF, Guidance for a Risk-Based Approach for Legal Professionals (2019) (see sections on STR reporting, tipping-off, and beneficial ownership).

10.6 Defence Against Money Laundering / Consent Requests

In certain circumstances, a legal professional may intend to carry out an act or transaction but know or suspect that it involves criminal property. Sections 133(2), 134(2) and 135(2) of POCA provide statutory defences where a disclosure is made to the FRA and the FRA's consent is obtained before the act is carried out. Where such circumstances arise, a SAR may include a DAML or consent request.

A SAR which includes a DAML/consent request must be clearly indicated as such.

Practical considerations when submitting a DAML or consent request are outlined in the FRA Industry Advisory: DAML/Consent Regime, issued 10 January 2025, which can be found on the FRA's website. In particular:

- A SAR that includes a DAML or consent request should be submitted via the AMLive portal or by secure email to FinancialReportingAuthority@gov.ky, ensuring that all relevant information is included.
- The SAR should clearly indicate that it is a "DAML SAR" and explain, in the "Reason for Suspicion" section, why consent is being sought and the activity for which consent is requested.
- The FRA operates a seven (7) working-day "Notice Period" (commencing on the first working day after submission). If the FRA does not respond within the Notice Period, consent is deemed to have been given (unless a longer period is specified because the request is incomplete).
- If consent is refused, a 30 calendar-day "Moratorium Period" applies (commencing on the first working day after refusal notice). The activity that is the subject of the request should not be carried out during the Moratorium Period.
- Legal professionals should remain mindful of the tipping off offence in section 139 of POCA when communicating with clients or third parties in relation to a SAR or DAML request.

10.7 Tipping Off and Prejudicing an Investigation

Legal professionals must ensure that internal and external disclosures are handled in a manner that prevents tipping off or prejudicing an investigation. Where information from a SAR is disclosed for the purposes of supervision or law enforcement, care is taken to ensure that the details concerning the reporting entity are not disclosed to other persons.

Where there are specific concerns regarding personal safety in relation to the making of a SAR, the matter should be raised with the FRA either within the report or by contacting the FRA at (345) 945-6267 or FinancialReportingAuthority@gov.ky. If there are concerns regarding immediate safety following the making of a SAR, or that the confidentiality of a SAR has been compromised, the Royal Cayman Islands Police Service should be contacted.

CHAPTER 11 – OTHER INTERNAL CONTROLS

11.1 Obligations under the AMLRs

Supervised Firms are required to establish, implement and maintain systems and controls that are comprehensive, effective and proportionate to the nature, scale and complexity of their activities and to the ML/TF/PF risks identified through their BRA. This obligation arises under regulation 5(a) of the AMLRs, which requires persons conducting RFB to maintain appropriate procedures, controls and risk-management measures to identify, assess, mitigate and manage the risks of ML/TF/PF. The minimum requirements are outlined in Chapter 4 of these Guidance Notes.

While obligations relating to AML/CFT/CPF policies and procedures are addressed throughout this Guidance, this Chapter focuses specifically on other internal controls that support, test and provide assurance on the effectiveness of the AML/CFT/CPF framework. In particular, it addresses internal controls relating to the establishment of an independent audit or review function, the governance and oversight of outsourcing and third-party arrangements, and employee screening procedures designed to ensure high standards of integrity, competence and suitability.

In accordance with regulation 5(a)(ix) and regulation 8 of the AMLRs, the nature, scope and intensity of these internal controls should be commensurate with the ML/TF/PF risks to which the Supervised Firm is exposed and with the size, structure and complexity of its operations.

11.2 Independent Audit Function

Regulation 5(a)(ix) of the AMLRs requires Supervised Firms to maintain “such other procedures of internal control, including an appropriate, effective risk-based independent audit function” for the ongoing monitoring of business relationships and transactions. The purpose of an independent audit function is to examine, evaluate and make recommendations regarding the adequacy and effectiveness of the Supervised Firm’s AML/CFT/CPF systems, policies and procedures, and to provide senior management with objective assurance that ML/TF/PF risks are being appropriately identified and managed.

An independent audit is distinct from routine compliance monitoring. Its purpose is not to perform operational compliance activities, but to provide independent challenge, testing and objective assurance as to the effectiveness of the firm’s AML/CFT/CPF framework.

11.2.1 Independence and Competence

The audit may be conducted by an internal or external party, provided that the individual or entity is independent of the functions being reviewed. Where an internal auditor is used, that person must not be involved in the design, implementation or day-to-day operation of the AML/CFT/CPF controls under review.

The auditor should have appropriate skills, experience and technical knowledge in AML/CFT/CPF and the legal and regulatory framework in the Cayman Islands. Where, in the course of an audit, the auditor forms knowledge or suspicion of ML/TF/PF, they must be prepared to escalate this internally in accordance with the firm’s internal reporting procedures.

Where an external auditor or consultant is engaged, the Supervised Firm should satisfy itself, through due diligence, that the auditor has suitable AML/CFT/CPF/financial crime expertise and experience relevant to the firm's size, services and risk profile.

11.2.2 Frequency, Scope and Methodology

The frequency of an independent audit should be determined using an RBA. While an annual audit may be appropriate for some Supervised Firms, others may justify a different frequency based on the nature and complexity of their activities, changes to their risk profile, or the outcomes of previous audits and supervisory interactions.

Higher-risk areas, clients, jurisdictions or services identified through the BRA should be subject to more frequent or targeted review. Sampling of client and matter files should be risk-based and sufficient to provide meaningful assurance across the Supervised Firm's activities.

11.2.3 Proportionality and Supervisory Expectations for Small Firms

In applying a risk-based approach, small Supervised Firms may determine that a formal independent AML/CFT/CPF audit is not necessary having regard to the nature, size and complexity of their business and their assessed ML/TF/PF risk exposure. The Supervised Firm should document the rationale for that determination and ensure that other proportionate measures are in place to periodically assess the effectiveness of its AML/CFT/CPF framework.

Where a small Supervised Firm makes a determination that an independent audit is not necessary, they may consider proportionate alternative measures, such as periodic external compliance reviews, peer reviews, or structured self-assessments benchmarked against regulatory requirements and supported by documented evidence. Small Supervised Firms should also ensure that any such reviews are conducted with sufficient objectivity and rigour, and that the scope, findings, remedial actions and follow-up steps are clearly documented and retained. Notwithstanding the above, the LSSA may determine that a Supervised Firm is required to undertake an independent AML/CFT/CPF audit where this is considered necessary having regard to the firm's risk profile, size, nature or complexity of its business, supervisory findings or compliance history.

11.2.4 Matters to be Assessed

An independent AML/CFT/CPF audit should include an assessment of whether:

- the firm's governance and oversight arrangements are appropriate to its size, structure and risk profile and are supported by an up-to-date BRA;
- AML/CFT/CPF policies and procedures are compliant with the AMLRs and supervisory guidance, tailored to the Supervised Firm's services, and effectively implemented in practice;
- roles, responsibilities and escalation arrangements are clearly defined and operating effectively;
- CDD, EDD and ongoing monitoring measures are risk-based, proportionate and consistently applied;
- higher-risk clients, matters, jurisdictions and services are subject to appropriate additional scrutiny and controls;

- SoF and SoW enquiries are undertaken and documented where required;
- internal controls operate effectively, including employee screening, training, outsourcing and record-keeping arrangements;
- TFS obligations are understood and complied with;
- staff knowledge and training are appropriate to their roles and reflected in day-to-day practices;
- records are complete, accurate, readily retrievable and retained in accordance with Part 8 of the AMLRs;
- issues identified through previous audits, reviews or supervisory interactions have been remediated in a timely and effective manner;

11.2.5 Documentation and Reporting

Supervised Firms should maintain clear written records of audits undertaken, including the scope and methodology, areas reviewed, findings, recommendations and remedial actions. Audit findings should be reported to senior management, and decisions taken in response, including reasons for not implementing recommendations, which should be documented and retained.

11.3 Employee Screening

Employee screening is a key preventive internal control required under regulation 5(a)(iii) of the AMLRs. It is designed to ensure that individuals in positions of trust are fit and proper and do not pose an ML/TF/PF risk to the Supervised Firm.

Screening should be conducted prior to appointment and on an ongoing basis thereafter, and should apply to all employees, particularly those whose roles are relevant to AML/CFT/CPF compliance, including partners, compliance staff and those involved in client onboarding, CDD, transaction handling or risk assessment.

Pre-employment screening should include verification of identity, qualifications and professional status, employment history and references, checks for regulatory or disciplinary action, criminal background checks, and adverse media searches. During employment, screening should be refreshed periodically, and may include fitness and propriety declarations, appraisal outcomes, training records and updated adverse information checks.

Screening measures should be proportionate, role-specific and risk-based, and all information collected must be handled securely and in accordance with applicable data protection legislation.

11.4 Outsourcing and Third-Party Arrangements

Supervised Firms may, as part of a proportionate and RBA, outsource certain aspects of their AML/CFT/CPF framework or engage third parties to provide compliance-related support, including compliance monitoring, advisory services, systems support, AMLCO or MLRO support functions. Such arrangements may be particularly appropriate for smaller practices or Supervised Firms without dedicated in-house compliance resources. However, outsourcing does not transfer regulatory responsibility, which remains at all times with the Supervised Firm, its partners and senior management.

Any outsourcing of AML/CFT/CPF-related activities should be subject to robust governance, effective internal controls and ongoing oversight, and must not undermine the Supervised Firm's ability to comply with its legal, regulatory or professional obligations, including duties of confidentiality and LPP.

Supervised Firms should maintain documented policies and procedures governing outsourcing and third-party arrangements. Prior to entering into any outsourcing arrangement, the Supervised Firm should conduct a risk assessment of the proposed arrangement, taking into account the nature and criticality of the outsourced activity, jurisdictional risk, confidentiality and data access risks, potential conflicts of interest, and the impact on the firm's ability to identify, manage and report ML/TF/PF risks. Where the risks associated with outsourcing cannot be effectively managed or mitigated, the Supervised Firm must not proceed with the arrangement.

Appropriate due diligence must be undertaken on any proposed outsourcing service provider prior to engagement and on an ongoing basis thereafter. This should include an assessment of the provider's competence, experience and expertise in AML/CFT/CPF matters relevant to legal services, their integrity and reputation, operational capacity, and, where applicable, their regulatory or professional standing. Supervised Firms must be satisfied that the service provider is fit and proper and capable of performing the outsourced activity to a standard equivalent to that required of the Supervised Firm itself.

Outsourcing arrangements should be governed by clear, written contractual agreements that define the scope and limitations of the outsourced services, reporting and escalation obligations, access rights, confidentiality and data protection requirements, audit and inspection rights, and the respective responsibilities of the parties. The Supervised Firm must retain timely and unrestricted access to all data, records, systems and outputs relevant to the outsourced activity and must not enter into outsourcing arrangements where access to information without delay may be impeded by confidentiality, secrecy, privacy or data protection restrictions.

Where AML/CFT/CPF activities are outsourced, the Supervised Firm should ensure that the service provider reports regularly and meaningfully in accordance with agreed timeframes and escalation protocols. The Supervised Firm should retain sufficient oversight to enable it to understand, challenge and, where necessary, override the service provider's conclusions. Arrangements must also support effective engagement with the LSSA and ensure that the Supervised Firm can respond promptly and fully to regulatory or law enforcement requests.

Supervised Firms should develop and maintain a contingency plan and exit strategy for outsourcing arrangements. This should include arrangements to ensure continuity of AML/CFT/CPF compliance in the event of service disruption, provider failure or termination of the arrangement, and should address the secure transfer or return of data and records.

Where outsourcing arrangements permit sub-contracting, the Supervised Firm must ensure that equivalent AML/CFT/CPF standards apply throughout the outsourcing chain. In particular, where a service provider or sub-contractor operates outside the Cayman Islands and is subject to lower AML/CFT/CPF standards, Cayman Islands-equivalent standards must be applied. The Supervised Firm should retain visibility over, and approval rights in respect of, any material sub-contracting.

Where knowledge or suspicion of ML/TF/PF arises in the course of performing outsourced activities, outsourcing arrangements must ensure that such matters are promptly escalated to the Supervised Firm in accordance with its internal reporting procedures. Where required, the service provider should be contractually obliged to support the Supervised Firm in the preparation and submission of SARs to the FRA, without breaching confidentiality or privilege.

Outsourcing and third-party arrangements should be reviewed periodically, and in any event resulting in a material change to the Supervised Firm's business model, risk profile, client base or regulatory obligations. The rationale for outsourcing, the scope of services, oversight arrangements and the ongoing effectiveness of the relationship should be documented and capable of being demonstrated to the LSSA upon request.

CHAPTER 12 – LEGAL PROFESSIONAL PRIVILEGE

12.1 Introduction

Legal professionals have a duty of full disclosure to their clients. However, there are certain circumstances in which there may be derogation from this rule. One key example is where disclosure to the client will result in tipping off. Section 139 of the POCA prohibits disclosure of certain information in circumstances where a SAR is required to be made. Notably, there are also other provisions of POCA and the AMLRs which adopt a similar approach.

This Chapter is intended to provide some insight into Legal Professional Privilege (LPP) as attorneys at law will need to give consideration to claims that may be made by their clients in respect of LPP and their obligations pursuant to POCA and the AMLRs.

Having read this chapter, if you are still unsure of your obligations and requisite actions to be taken, you should seek independent legal advice.

12.2 Duty of Confidentiality

A legal professional is professionally and legally obliged to keep the affairs of clients confidential and to ensure that his or her staff also maintains that confidentiality. The obligations extend to all matters revealed to a legal professional, from whatever source, by a client, or someone acting on the client's behalf.

In exceptional circumstances, this general duty of confidentiality may be overridden. However, there are certain communications and material evidencing same that can never be disclosed unless statute permits this either expressly or by necessary implication; such communications include those protected by LPP (unless waived).

12.3 LPP

12.3.1 General Overview

LPP recognises the client's fundamental human right to be candid with his or her legal adviser, without fear of later disclosure resulting in prejudice. It is an absolute right and cannot be overridden by any other interest.

It is essential to remember that LPP does not extend to every communication, information and material that legal professionals have a duty to keep confidential. LPP protects only those confidential communications and material evidencing same which falls under either of the two types of LPP –

- 1) Legal advice privilege
- 2) Litigation privilege.

Attorneys should consider seeking specific legal advice based on their circumstances should it appear that LPP may apply.

12.3.2 Legal Advice Privilege

Principle

Communications between a legal professional and a client, are protected by LPP if they are both:

- confidential; and
- for the primary purpose of seeking or providing legal advice.

Scope

Communications are not privileged merely because a client is speaking or writing to you. The protection applies only to those communications which directly seek or provide legal advice or which are given in a legal context, that involve the legal professional using his or her legal skills and which are directly related to the performance of the legal professional's professional duties [*Passmore on Privilege 2nd edition 2006*].

English case law helps define what legal advice privilege covers. Communications subject to legal advice privilege:

- a solicitor's bill of costs and statement of account [*Chant v Brown* (1852) 9 Hare 790]; and
- information imparted by prospective clients in advance of a retainer if the communications were made for the purpose of indicating the advice required [*Minster v Priest* [1930] AC 558 per Lord Atkin at 584].

Communications not subject to advice privilege:

- notes of open court proceedings [*Parry v News Group Newspapers* (1990) 140 New Law Journal 1719], as the content of the communication is not confidential;
- conversations, correspondence or meetings with opposing legal professionals [*Parry v News Group Newspapers* (1990) 140 New Law Journal 1719], as the content of the communication is not confidential;
- a client account ledger maintained in relation to the client's money [*Nationwide Building Society v Various Solicitors* [1999] P.N.L.R. 53.];
- an appointments, diary or time record or an attendance note, time sheet or fee record relating to a client [*R v Manchester Crown Court, ex p. Rogers* [1999] 1 W.L.R. 832]; and
- conveyancing documents, as they are not communications [*R v Inner London Crown Court ex p. Baines & Baines* [1988] QB 579].

Advice within a Transaction

All communications between a legal professional and his or her client relating to a transaction in which the legal professional has been instructed for the purpose of obtaining legal advice are covered by legal advice privilege, notwithstanding that they do not contain advice on matters of law and construction, provided that they are directly related to the performance by the legal professional of

his or her professional duty as legal adviser of his or her client. [*Three Rivers District Council and others v the Bank of England* [2004] UKHL 48 at 111].

This means that where you are providing legal advice in a transactional matter (such as a conveyance) the advice privilege will cover all:

- communications with,
- instructions from, and
- advice given to the client, including any working papers and drafts prepared, as long as they are directly related to your performance of your professional duties as a legal adviser.

12.3.3 Litigation Privilege

Principle

This privilege, which is wider than legal advice privilege, protects confidential communications made after litigation has started, or is reasonably in prospect, between any of the following:

- a legal professional and a client;
- a legal professional and an agent, whether or not that agent is a legal professional; or
- a legal professional and a third party.

These communications must be for the sole or dominant purpose of litigation, for any of the following:

- seeking or giving legal advice in relation to it;
- obtaining evidence to be used in it; or
- obtaining information leading to obtaining such evidence.

12.3.4 Important Points to Consider

An original document not brought into existence for these privileged purposes and so not already privileged, does not become privileged merely by being given to a legal professional for advice or other privileged purpose.

Further, where you have a corporate client, communication between you and an employee of a corporate client may not be protected by LPP if the employee cannot be considered to be 'the client' for the purposes of the retainer. As such, some employees will be clients, while others will not. [*Three Rivers District Council v the Governor and Company of the Bank of England (no 5)* [2003] QB 1556]

It is not a breach of LPP to discuss a matter with your Nominated Officer for the purposes of receiving advice on whether to make a disclosure.

12.3.5 Crime/Fraud Exception

LPP protects advice you give to a client on avoiding committing a crime [*Bullivant v Att-Gen of Victoria* [1901] AC 196] or warning a client that proposed actions could attract prosecution [*Butler v Board of Trade* [1971] Ch 680]. LPP does not extend to documents which themselves form part of a criminal or

fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence [*R v Cox & Railton* (1884) 14 QBD 153]. It is irrelevant whether you are aware that you are being used for that purpose [*Banque Keyser Ullman v Skandia* [1986] 1 Lloyd's Rep 336].

Intention of Furthering a Criminal Purpose

It is not just your client's intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the legal professional/client communication to be made with that purpose (e.g. where the innocent client is being used by a third party) [*R v Central Criminal Court ex p Francis & Francis* [1989] 1 AC 346].

Knowing a Transaction Constitutes an Offence

If you know the transaction you are working on is a principal offence, you risk committing an offence yourself. In these circumstances, communications relating to such a transaction are not privileged and should be disclosed.

Suspecting a Transaction Constitutes an Offence

If you merely suspect a transaction might constitute an ML offence, the position is more complex. If the suspicions are correct, communications with the client are not privileged. If the suspicions are unfounded, the communications should remain privileged and are therefore non-disclosable.

Prima Facie Evidence

If you suspect you are unwittingly being involved by your client in a fraud, the courts require prima facie evidence before LPP can be displaced [*O'Rourke v Darbishire* [1920] AC 581]. The sufficiency of that evidence depends on the circumstances. It is easier to infer a prima facie case where there is substantial material available to support an inference of fraud. While you may decide yourself if prima facie evidence exists, you may also ask the court for directions [*Finers v Miro* [1991] 1 W.L.R. 35].

If a legal professional forms a genuine, but mistaken, belief that the privileged circumstances exemption (see 12.4 below) applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence. It is likely that a similar approach would be taken with respect to a genuine, but mistaken, belief that LPP applies.

12.4 Privileged Circumstances

The POCA recognises another type of communication, one which is received in 'privileged circumstances'. Whilst this is not the same as LPP, the privileged circumstances exemption is found in the following legislation:

- POCA – Sections 133(4), 134(2)(c), 135(2)(c), 136(2)(b) and 137(2)(b).

TA – Sections 17(2), 23(6), Schedule 1, 1(5). Although the wording is not exactly the same in all these sections, the essential elements of the exemption are:

- you are a professional legal adviser;
- the information or material is communicated to you:

- i. by your client or their representative in connection with you giving legal advice;
- ii. by your client or their representative in connection with its seeking legal advice from you; or
- iii. by any person for the purpose of or in connection with actual or contemplated legal proceedings; and
- the information or material cannot be communicated or given to you with a view to furthering a criminal purpose.

The defence covers legal professional advisers and their employees.

Consider the crime/fraud exception when determining what constitutes the furthering of a criminal purpose.

12.5 Differences between privileged circumstances and LPP

12.5.1 Protection of Advice

When advice is given or received in circumstances where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances, communications between you and third parties will not be protected under the advice arm of LPP.

Privileged circumstances, however, exempt communications regarding information communicated by representatives of a client, where it is in connection with you giving legal advice to the client, or the client seeking legal advice from you. This may include communications with:

- a junior employee of a client (if it is reasonable in the circumstances to consider that employee to be a representative of the client); or
- other professionals who are providing information to you on behalf of the client as part of the transaction.

You should consider the facts of each case when deciding whether a person is a representative for the purposes of privileged circumstances.

12.5.2 Losing Protection by Dissemination

There may be circumstances in which a legal adviser has received information which is subject to LPP, but which does not fall within the definition of privileged circumstances.

For example, a legal professional representing client A may hold or have had communicated to him or her information which is privileged as between client B and his or her own legal professional, in circumstances where client A and client B are parties to a transaction, or have some other shared interest.

The sharing of this information may not result in client B's privilege being lost, if it is stipulated that privilege is not waived (*Gotha City v Sotheby's* (no1) [1998] 1 WLR 114).

Privileged circumstances will not apply because the information was not communicated to client A's legal professional by a client of that professional in connection with the giving by him of legal advice to that client. However, if it was given to him or her by any person in connection with legal proceedings or contemplated legal proceedings, privileged circumstances would apply.

In such circumstances, the legal professional representing client A would not be able to rely on privileged circumstances, but the information might still be subject to LPP, unless the crime/fraud exemption applied.

12.5.3 Vulnerability to Seizure

It is important to correctly identify whether communications are protected by LPP or if they are merely covered by the privileged circumstances exemption. This is because the privileged circumstances exemption relieves you from liability under certain POCA provisions. It does not provide any of the other LPP protections to those communications.

Therefore, a communication which is only covered by privileged circumstances, not LPP, will remain vulnerable to seizure or production under a court order or other such notice from law enforcement agencies.

12.6 When do you Disclose?

If the communication is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under the POCA.

If the communication was received in privileged circumstances and the crime/fraud exception does not apply, you are exempt from the relevant provisions of the POCA, which includes making a disclosure to the FRA.

If neither of these situations applies, the communication will still be confidential, however, the material should be disclosed pursuant to the relevant provisions of POCA.



info@caymanlssa.ky
www.caymanlssa.ky