The Turks and Caicos Islands Financial Services Commission

Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism for Accountancy Sectors

Issued October 2013

Sector Specific Guidance for the Accountancy Sector

Contents

1 Introduction

Criminals have responded to the anti-money laundering and prevention of financing measures taken by the traditional financial sector over the past decade and have sought other means to convert their proceeds of crime. Professionals such as accountants have, in some jurisdictions, been used as a conduit for criminal property to enter the financial system.

The accountancy sector in the Turks and Caicos Islands should be on guard to ensure that it is not used as such a conduit. In particular, criminals and money launderers may try to exploit the services offered by accountants, through the business of undertaking financial transactions.

In response to the changing landscape of money laundering and terrorist financing, inter-governmental and international standard setting organisations, notably the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF) styled body have extended the scope of recommended prevention measures. FATF recommendations now include Anti-Money Laundering and Combating Terrorist Financing responsibilities to a group of businesses and professions collectively named as Designated Non Financial Businesses and Professions. (Referred to as DNFBP).

The FATF, has found that globally accountants are susceptible to being used not only in the layering and integration stages of money laundering, as has been the case historically, but also as a means to disguise the origin of funds before placing them into the financial system. Accountants are often the first professionals consulted for financial advice.

The FATF characterises accountants as “Gatekeepers” because they “protect the gates to the financial system,” through which potential users must pass in order to succeed. The term also includes professional experts who provide financial expertise to launderers, such as, lawyers, accountants, tax advisers, and trust and service company providers. The FATF has noted that gatekeepers are a common element in complex money laundering schemes. Gatekeepers’ skills are important in identifying legal structures that could be used to launder money and for their ability to manage and perform transactions efficiently and to avoid detection.

In the Turks and Caicos Islands DNFBPs encompass Accountants, Real Estate Agents, independent legal professionals, and Dealers in High Value Goods.

As a well-regulated jurisdiction operating in the international financial arena, the Turks and Caicos Islands has adopted the international standards to guard against money laundering and terrorist financing and has integrated the requirements into the legal and regulatory system.

Accountants are key professionals in the business and financial world, facilitating vital financial transactions that underpin the Turks and Caicos Islands economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activity.

The continuing ability of the Turks and Caicos Islands financial services industry to attract legitimate clients with funds and assets that are clean and untainted by criminality depends, in large, upon the Island’s reputation as a sound, well-regulated jurisdiction. Any accountant in the Turks and Caicos Islands that assists in laundering the proceeds of crime, or financing of terrorism, whether:

- with knowledge or suspicion of the connection to crime; or
- in certain circumstances, acting without regard to what it may be facilitating through the provision of its services,

will face the loss of its reputation, and damage the integrity of the Turks and Caicos Islands professional and financial services industry as a whole, and may risk prosecution for criminal

offences.

2 Purpose of this Guidance Document

The purpose of this document is to provide industry specific guidance for accountants on their legal obligations to deter and detect money laundering and financing of terrorism activities.

Reference is made throughout this document to AML/PTF and AML/CTF. See Glossary at the end of this document. The Regulations refer to Anti Money Laundering and Prevention of Terrorist Financing and other bodies tend to use AML/CTF - Anti Money Laundering and Countering (or Combating) of Terrorist Financing. The two pieces of terminology are interchangeable

3 Status of this guidance

The objective of this guidance document is to supplement, with specific reference to the accountancy profession, the detailed guidance and reference to The Proceeds of Crime Ordinance, ("The POCO") The Anti-Money Laundering and Prevention of Terrorism Regulations 2010 ("The Regulations") and the Anti-Money Laundering and Prevention of Terrorist Financing Code 2010. ("The Code").

In case of doubt between this document and The Code, The Code will take precedence.

This guidance uses plain language to explain the most common situations under the specific laws and related regulations which impose AML/PTF requirements. It is provided as general information only. It is not legal advice, and is not intended to replace The POCO or to replace the Regulations.

This guidance is intended for use by senior management and compliance staff of an accountancy firm to assist in the development of systems and controls. It is not intended to be used by accountancy firms as an internal procedures manual.

4 The Turks and Caicos Islands Financial Services Commission as the Supervisory Authority.

The Turks and Caicos Islands Financial Services Commission (The Commission) has the role required by the Regulations to supervise the effectiveness of the anti-money laundering regime for DNFBP. The Regulations seek to reduce businesses' vulnerability to being used for money laundering or terrorist financing.

In accordance with Regulation 23 of the Regulations, The Commission has been appointed the sole supervisory authority of all DNFBP for the purposes of Section 148F (2) of the POCO

As the Supervisor, the Commission is required to:

- Establish and maintain a Register of all DNFBPs.
- Monitor compliance with the Regulations.
- Take appropriate enforcement action.

5 Businesses and Individuals within the scope of this guidance

5.1 To whom do these obligations apply?

5.1.1 Introduction

The Regulations Schedule 2 (1) (f) (i) refers to a Designated Non Financial Business and Profession to be a business which by way of business provides accountancy or audit services.

These obligations apply to accountants operating in the Turks and Caicos Islands.

5.1.2 Accountancy Services

Accountancy services include any service provided under a contract for services (i.e. not a contract of employment) which pertains to the recording, review, analysis calculation or reporting of financial information.

5.1.3 Audit Services

The use of the term “auditor” in these Guidance Notes means anyone who is part of the engagement team (not necessarily only those employed by an audit firm). The engagement team comprises all persons who are directly involved in the acceptance and performance of a particular audit. This includes the audit team, professional personnel from other disciplines involved in the audit engagement and those who provide quality control or direct oversight of the audit engagement. However it does not include experts contracted by the firm.

The extent to which money laundering legislation affects the auditors work differs between two broad categories of audit:

5.1.3.1 Audit of regulated or licenced businesses.

Regulated or licenced firms are required to comply with the requirements of the AML/PTF Regulations which place obligations on them to combat money laundering and terrorist financing. All such businesses are required to comply with the regulatory requirements and best practice guidelines issued by the Commission

In addition to reporting on their financial statements, auditors of licenced businesses are expected to report to the Commission on matters of significance that come to their attention in the course of their work, including compliance with relevant legislations, directives, internal policies and procedures and guidelines.

Therefore auditors of such businesses should not only be aware of the key provisions contained in the AML/PTF Regulations as they affect auditors themselves, but also the requirements of the relevant AML/PTF Regulations covering the business that they are auditing.

5.1.3.2 Audits of other type of entity

In general, auditors of other types of entity not covered by the AML/PTF Regulations are required only to take appropriate steps in response to factors encountered in the course of their work which lead them to suspect that money laundering or terrorist financing is taking place.

Auditors need to take the possibility of money laundering and terrorist financing into account in the course of carrying out procedures relating to fraud and compliance with the money laundering legislation. An auditor's wide access to documents and systems and the need to understand the business, can make then ideally suited to spot such issues as they arise.

5.2 Obligations under the Regulations

As an accountant the main obligations under the AML/CFT Regulations are summarized below:

1. Register with the Financial Services Commission;
2. Submit Suspicious Activity Reports to the Financial Intelligence Unit;
3. Avoid "Tipping-off";
4. Keep Records;
5. Ascertain client identity;
6. Establish Source of funds and where necessary Sources of Wealth
7. Ascertain whether the client is acting for a Third Party;
8. Appoint a Money Laundering Compliance Officer;
9. Appoint a Money Laundering Reporting Officer;
10. Develop an effective Compliance Programme and
11. Implement the Compliance Programme and conduct periodic reviews.

6 What is Money Laundering?

Money Laundering is the process by which funds derived from criminal activity ("dirty money") are given the appearance of having been legitimately obtained, through a series of transactions in

which the funds are 'cleaned'. Its purpose is to allow criminals to maintain control over those proceeds and, ultimately, provide a legitimate cover for the source of their income.
For money laundering to take place, first, there must have been the commission of a serious crime[1] which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies.

There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewellery) to passing money through legitimate businesses and "shell" companies.

6.1 The Stages of Money Laundering

The money laundering process is generally described as taking three stages. It is important to remember that the three stages are not necessarily sequential. For example the laundering of the proceeds of corruption typically commences at the layering stage as the proceeds are already in the banking system and diverted through layering out of the hands of the rightful owner.

6.1.1 Placement

Criminally derived funds are brought into the financial system. In the case of drug trafficking, and some other serious crimes, such as robbery, the proceeds usually take the form of cash which needs to enter the financial system. Examples of Placement are depositing cash into bank accounts or using cash to purchase assets. Techniques used include Structuring - breaking up a large deposit transaction into smaller cash deposits and Smurfing – using other persons to deposit cash.

6.1.2 Layering

This takes place after the funds have entered into the financial system and involves the movement of the funds. Funds may be shuttled through a complex web of multiple accounts, companies, and countries in order to disguise their origins. The intention is to conceal, and

[1] Also referred to as a Predicate Crime

obscure the money trail in order to deceive LEAs and to make the paper trail very difficult to follow.

6.1.3 Integration

The money comes back to criminals “cleaned”, as apparently legitimate funds. The laundered funds are used to fund further criminal activity or spent to enhance the criminal's lifestyle. Criminals may use your services to assist in investment in legitimate businesses or other forms of investment, to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities.
Successful money laundering allows criminals to use and enjoy the income from the criminal activity without suspicion.

7 What is Financing of Terrorism?

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity. Funds may involve low dollar value transactions and give the appearance of innocence and a variety of sources. Funds may come from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organise fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, all the funds are actually transferred to a terrorist group. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.
Unlike money laundering, which precedes criminal activity, with financing of terrorism you may have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place.
However, like money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. The reason is to prevent leaving a trail of incriminating evidence - to distance the funds from the crime or the source, and to obscure the intended destination and purpose.

8 Legislation

This section provides a brief overview only of the legislation and regulations.

8.1 Legislation, Regulations and The Code

The Proceeds of Crime Ordinance was amended in 2009, 2010, 2011, and 2013.

- Proceeds of Crime Ordinance Chapter 3.15 (as amended) (The Principal Ordinance)
- The Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010
- The Anti-Money Laundering and Prevention of Terrorist Financing Code 2011

8.2 Money Laundering Offences

Money Laundering is dealt with in Part IV Sections 108 – 125 of the Proceeds of Crime Ordinance (POCO)

Establishment Operations and Functions of the Money Laundering Reporting Authority.	**Sections 108 – 114**
Criminal Property	Section 115 – 116
Offences of Concealing, Disguising, Converting, Transferring and removing Criminal Property	Section 117
Offence of Arrangements	Section 118
Offences of Acquisition and Possession of Criminal Property	Section 119
Duty to Disclose Knowledge or Suspicion of Money Laundering	Sections 120 – 122
Offence of Prejudicing Investigations and Tipping Off	Section 123 – 124

8.2.1 Non Compliance with Money Laundering Regulations

Non-compliance with obligations under the AML/CFT laws and regulations may result in criminal and or administrative sanctions.

Penalties include fines and terms of imprisonment, and sanctions include possible revocation of licenses, issuance of directives and court orders.

9 Registration with the Financial Services Commission

9.1 Registration Procedure

Applicants for registration must complete and submit a paper copy of the Application to Register.

The application form is available on the Financial Services Commission website. The form may be prepared electronically and printed.

Applicants are strongly advised to refer to the Guidance Notes to Registration available on the website.

An advance copy of the Application to register may be submitted by email to the address dnfbp@tcifsc.tc

- A signed paper printed copy of the Application to Register together with supporting documents must be delivered by hand to either the Providenciales or Grand Turk offices of the Commission.

9.1.1 Supporting Documents

The Application to register and the Guidance Notes describe the documents which must be provided to verify information.

Every effort will be made by the Commission to reduce the amount of verification documentation which must be provided, wherever possible, by utilising information and documentation already provided or available to the Commission.

Documents which must be submitted as verification must be certified by one of; a Notary Public, Justice of the Peace, or Commissioner of Oaths, as a true copy of the original.

9.1.2 Receipt of Registration Application by the Commission

The Commission undertakes to acknowledge receipt within two working days of receiving the Application to Register.

The Commission will advise by a letter to the applicant within 30 days of receipt, of the outcome of the application unless additional information is requested. The response shall be one of:

- Registration Confirmed.
- Registration Refused.
- A request for further information or documentation. (In such cases the Commission shall keep the applicant advised of progress.

9.1.3 Refusal of a request for registration

A refusal of the Application will be in written form and will state the grounds for refusal.

The grounds upon which the Commission may refuse an Application for Registration are one or more than one of the following criteria:

a) The applicant does not comply with Regulation 25.

b) The applicant fails to provide any information or documents required by the Supervisor under Regulation 25 (3)

c) The Supervisor is of the opinion that –

- The applicant does not intend to carry on the relevant business for which it seeks registration.

- The business or any of its directors, senior officers or owners does not satisfy the Supervisors fit and proper criteria.

- It is contrary to the public interest for the business to be registered.

For full details of grounds for refusal please refer to the Regulations.

9.1.4 Registration refused: Right to Appeal

In the event that an Application to Register is refused, the applicant may submit an appeal addressed to the Managing Director of the Commission, and submitted by email to;

dnfbp@tcifsc.tc

9.1.5 Forms

The following forms are must be used and can be accessed by following the link in the FSC website.

9.1.6 Continuing Registration and Material Changes

Subsequent to the initial submission, registration is an on-going process. Renewals of existing successful applications will take place on the third anniversary of the original approval, i.e. Registration is valid for a three year period.

All individuals and businesses are required to register as soon as they begin to provide the services designated for their business or profession.

If at any time after registration there are material changes to the information supplied as part of the application, or it becomes apparent that there is a significant inaccuracy in the details provided, the business must notify the Commission within 30 days of the changes occurring or the inaccuracy being discovered.

If a business does not notify the Commission of any material changes or inaccuracies in the details provided for registration, it will be in breach of the Regulations and may be subject to civil penalties or prosecution.

9.1.7 Offence - Failure to Register

A business shall not carry out a relevant business as a Designated Non Financial Business and Profession until registered with the FSC.[2]

Failure to register when required may result on summary conviction to imprisonment for a term of twelve months, or a fine of $20,000 or both. On conviction on indictment to imprisonment for a term of three years or to a fine of $75,000 or to both.

10 Anti-Money Laundering Systems and Controls

10.1 Corporate Governance

Corporate governance is the system by which businesses are directed and controlled and the business risks managed. Money laundering and terrorist financing are risks that must be managed in the same way as other business risks.

10.2 Responsibilities of the Board

It is the responsibility of the Board, or senior management, or the owner(s) to ensure that the organisational structure of the business effectively manages the risks it faces.

Section 5 of the Code provides the principal responsibilities of the Board. Senior Management, the Money Laundering Compliance Officer and the Money Laundering Reporting Officer. will assist the Board in fulfilling these responsibilities.

[2] POCO Sections 148H (1) and (2)

Larger and more complex firms may also require dedicated risk and internal audit functions to assist in the assessment and management of money laundering and terrorist financing risk.

10.3 Policies, systems and controls[3]

10.3.1 Establish and maintain systems and controls

A firm must establish and maintain systems and controls to prevent and detect money laundering and terrorist financing that enable the business to;

- Apply appropriate client due diligence (CDD) policies and procedures that take into account vulnerabilities and risk. Policies and procedures must include;
    - The development of clear client acceptance policies and procedures and
    - Identifying and verifying the identity of the applicant of the business.
- Monitor and review instances where exemptions are granted to policies and procedures or where controls are overridden.
- Report to the Turks and Caicos Islands Financial Intelligence Unit when it knows or has reasonable grounds to know or suspect that another person is involved in money laundering or terrorist financing, including attempted transactions.
- Ensure that relevant employees are
    - adequately screened when they are initially employed,
    - aware of the risks of becoming concerned in arrangements involving criminal money and terrorist financing,
    - aware of their personal obligations and the internal policies and procedures concerning measures to combat money laundering and terrorist financing, and
    - provided with adequate training.
- Maintain adequate records
- Liaise closely with the Commission and the FIU on matters concerning vigilance, systems and controls.

[3] The Code Part 2

In maintaining the required systems and controls, a firm must ensure that the systems and controls are implemented and operating effectively.

A firm must also have policies and procedures in place to address specific risks associated with non Face to Face business relationships or transactions, which should be applied when conducting due diligence procedures.

10.3.2 Internal Controls

The level of internal controls, and the extent to which monitoring needs to take place will be affected by

- The firm's size
- The nature and the scale of the practice and
- The overall risk profile

Issues which may be covered in an internal controls system include;

- The level of personnel permitted to exercise discretion on the risk based application of regulations and under what circumstances.
- CDD requirements to be met for simplified, standard and enhanced due diligence.
- When outsourcing of CDD obligations or reliance upon third parties will be permitted and under what conditions.
- How the firm will restrict work being conducted on a file where CDD has not been completed.
- The circumstances in which delayed CDD is permitted.
- When cash payments will be accepted.
- When payments will be accepted from or made to third parties
- The manner in which disclosures are to be made to the MLRO.

10.3.3 Monitoring Compliance

Monitoring compliance will assist a firm to assess whether the policies and procedures that have been implemented are effective in managing the risk of money laundering and terrorist financing.

Procedures to be undertaken to monitor compliance may involve

- Random file audits.
- File checklists to be completed before opening or closing a file.
- An MLRO's log of situations brought to their attention including queries from staff and reports made.
- How the firm rectifies lack of compliance when identified.
- Hoe lessons learnt will be communicated back to staff and fed back into the risk profile of the firm.
- All employees involved in the day-to-day business of a firm should be made aware of the policies and procedures in place in their firm to prevent money laundering and financing of terrorism risks. It is essential for businesses to evaluate compliance by staff with policies and procedures, in particular, CDD record keeping and suspicious transactions reporting. Best practice indicates that internal testing should be carried out by someone other than the Compliance Officer, to avoid potential conflict since the Compliance Officer is responsible for implementation of the Compliance Programme, its measures and controls.
- If the Compliance Officer is also the most senior employee (person at the highest level in the organization) additional care must be exercised to test compliance with your obligation in respect of AML/CFT obligations.
- Such reviews (whether they may be internal or external) must be documented and made available to the Financial Services Commission.

10.3.4 Compliance programme

After a firm has registered with the FSC, a written Compliance Programme must be developed. If an organization, the Compliance Programme also has to be approved by senior management.

The Compliance Programme is a written document explaining the system of internal procedures, systems and controls which are intended to make the business less vulnerable to money

laundering and the financing of terrorism. The Compliance Programme encapsulates the guidance provided in the section policies, systems and controls.

These policies, procedures and controls, must be communicated to employees, and fully implemented.

The Compliance Programme must be reviewed at a minimum of every two years, or more frequently if the initial and on-going business risk assessment warrants or if there are changes to Legislation, Regulations or The Code.

A well-designed, applied and monitored regime will provide a solid foundation for compliance with the AML/CFT laws. As not all individuals and entities operate under the same circumstances, compliance procedures will have to be tailored to fit individual needs. It should reflect the nature, size and complexity of the operations as well as the vulnerability of the business to money laundering and terrorism financing activities.

11 Risk Based Approach[4]

11.1 Overview

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

The possibility of being used to assist with money laundering and terrorist financing poses many risks to accountancy businesses including;

- Criminal and disciplinary sanctions for firms and for individual accountants
- Civil action against the firm as a whole and against individual partners.
- Damage to reputation leading to loss of business.

[4] Reference the guidance provided in Part II of the Code.

These risks must be identified and mitigated as any other risk which the business faces.

Such an approach;

- Recognises that the money laundering and terrorist financing threats to an accountant cross clients, jurisdictions, services and delivery channels.
- Allows firms to differentiate between clients in a way that matches risk in a particular business.
- While establishing minimum standards, allows an accountant to apply its own approach to systems and controls and other arrangements in particular circumstances
- Helps to produce a more cost effective system.

A firm is expected to conduct and keep up to date a Business Risk Assessment, which considers the business activities and structure and concludes on the firm's exposure to money laundering and terrorist financing risk. The firm must use the outcome of the risk assessment in the development of appropriate risk management systems and controls and the business's policies and procedures.

Once risks are understood businesses may apply AML/PTF measures in a way that ensures they are commensurate with those risks, assisting in prioritisation and the efficient use of resources.

Firms must develop CDD[5] procedures that take into account risk and to apply enhanced CDD procedures to higher risk[6] client relationships. Simplified due diligence can also be applied in circumstances where the money laundering risk is considered to be at its lowest.

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

Accountants may extend its existing risk management systems to address money laundering and terrorist financing risks. The detail and sophistication of these systems will depend on the size and the complexity of the business it undertakes. Ways of incorporating a firms' business risk assessment will be governed by the size of the firm and how regularly compliance staff and

[5] See Glossary
[6] Part III of the Code.

senior management are involved in day-to-day activities.

11.2 Business Risk Assessment: Key Concepts

The business risk assessment will depend on the firm's size, type of clients and the practice area it engages in.
This section addresses the Business Risk Assessment at the portfolio level of the firm. Accounting businesses are also encouraged to consider Money Laundering and Terrorist financing risk at the client level.

A risk assessment views risk as a function of three factors, threat, vulnerability and consequence.

11.2.1 Threat

A threat is a person, group of people, an activity or object which may do harm to the business. In the Money Laundering/Terrorist Financing context this includes criminals, terrorist groups, and their facilitators.

11.2.2 Vulnerabilities

In risk assessment vulnerability comprise those things that can be exploited by the threat or that may support or facilitate those activities.

Looking at vulnerabilities as distinct from threat means focussing upon the factors that represent weaknesses in Anti Money Laundering and Prevention of Terrorist Financing systems or controls, for example a particular service or product which has certain features which make them attractive for Money Laundering or Terrorist Financing purposes.

11.2.3 Consequence

Consequence refers to the impact or harm that Money Laundering or Terrorist Financing may cause. The consequences may be short or long term, ranging from prosecution of the individuals concerned, reputational damage to the firm or forfeiture of laundered assets.

Assessing consequence may be challenging, given the lack of clear data and experiences. It is not always necessary to assess consequence in a sophisticated manner, but a high level understanding of the impacts and consequences should be assessed as a benchmark of what may happen.

The key is that any risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist in prioritising mitigation efforts.

11.2.4 Sources of risk

Sources may be organised into three groupings described below.

It is important to recognise that this section looks at the portfolio level of risk assessment. A separate section in the Handbook looks at client level risk assessment.

11.2.4.1 Country / Geographic Risk

There is no universally agreed definition that prescribes whether a particular country or geographic area represents a higher risk. Country risk in conjunction with other risk factors provides useful information as to potential money laundering and terrorist financing risks. Money laundering and terrorist financing risks have the potential to arise from almost any source, such as the domicile of the client, the location of the transaction, and the source of the funding. Countries that pose a higher risk include.

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN) and OFAC[7]. In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but that may not be universally recognised, may be taken into consideration by a firm because of the standing of the issuer of the sanctions and the nature of the measures.

[7] See Glossary

- Countries identified by credible sources[8] as generally lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as being a location from which funds or support are provided to terrorist organizations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.

11.2.4.2 Client Risk

Determining the potential money laundering or terrorist financing risks posed by a client, or category of clients, is critical to the development and implementation of an overall risk-based framework. Based on its own criteria, a firm should seek to determine whether particular types or categories of client pose a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment.

Categories of clients whose activities may indicate a higher risk include:

- Politically Exposed Persons[9] (PEPs) are considered as higher risk clients – If an accountant is advising a client that is PEP, or where PEP is the beneficial owner (BO) of the client, and then it is necessary to carry out appropriate enhanced Client Due Diligence. (CDD). Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's home country, the type of work the PEP is instructing the firm to perform or carry out, and the scrutiny to which the PEP is under in the PEPs home country.
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely fashion the true beneficial owner or controlling interests, such as the unexplained use of legal persons or legal arrangements, nominee shares or bearer shares.

[8] Credible sources refer to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publically and widely available. In addition to the FATF and FATF styled regional bodies such sources may include but are not limited to, supra-national; or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

[9] See section of the Handbook 12.2 – Politically Exposed Persons

- Clients that are cash (and cash equivalent) intensive businesses.

There are many other situations which may constitute higher risk and reference should be made to the "red flags" section of this Handbook together with the client level risk profiling adopted by the business.

11.2.4.3 Service Risk

An overall risk assessment should also include determining the potential risks presented by the services offered by an accountant. The context of the services being offered or delivered is always fundamental to a risk-based approach. Any one of the factors discussed in this Guidance alone may not itself constitute a high risk circumstance. High risk circumstances can be determined only by the careful evaluation of a range of factors that cumulatively and after taking into account any mitigating circumstances would warrant increased risk assessment. When determining the risks associated with provision of services related to specified activities, consideration should be given to such factors as:

- Services where accountants are acting with other financial intermediaries.
- Services which conceal improperly beneficial ownership from competent authorities.
- Services requested by the client for which the accountant does not have expertise.
- Payments proposed from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

11.2.5 Variables which may Impact Risk

Due regard must be accorded to the vast and profound differences in, size, scale and expertise, amongst accountancy firms. As a result, consideration must be given to these factors when creating a reasonable risk-based approach and the resources that can be reasonably allocated to implement and manage it. For example, a sole practitioner accountant would not be expected to devote an equivalent level of resources as a large practice firm; rather, the sole practitioner

would be expected to develop appropriate systems and controls and a risk-based approach proportionate to the scope and nature of the practice.

A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular firm. This factor must always be considered in the context of the type of business. A risk-based approach methodology may thus take into account risk variables specific to a particular client or type of work. Consistent with the risk-based approach and the concept of proportionality, the presence of one or more of these variables may cause an accountant to conclude that either enhanced due diligence and monitoring is warranted, or conversely that normal CDD and monitoring can be reduced, modified or simplified. These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

- The level of regulation or other oversight or governance regime to which a client is subject. For example, a client that is a financial institution or regulated in a country with a satisfactory AML/CFT regime poses less risk of money laundering than a client in an industry that has money laundering risks and yet is unregulated for money laundering purposes.
- The reputation and publicly available information about a client. Legal persons that are transparent and well known in the public domain and have operated for a number of years without being convicted of proceeds generating crimes may have low susceptibility to money laundering.

11.3 Money Laundering Compliance Officer and Money Laundering Reporting Officer.[10]

11.3.1 Overview

Section 8 of the AML Code provides detailed explanation of the roles of the responsibilities of the Money Laundering Compliance Officer (MLCO) and Money Laundering Reporting Officer. (MLRO)

[10] Part II Sections 8 and 9 of the Code.

The MLCO is required to

- Develop and maintain systems and controls (including policies and procedures) for both Anti Money Laundering and Prevention of Terrorist Financing in line with evolving requirements;
- Undertake regular reviews (including testing) of compliance with policies and procedures to counter money laundering and the financing of terrorism;
- Report periodically to and advise senior management on anti-money laundering and terrorist financing compliance issues that need to be brought to its attention;
- Respond promptly to requests for information made by the Commission.

The MLRO is required to:

Assess internal suspicious activity reports and submit suspicious activity reports when required to the Turks and Caicos Islands Financial Intelligence Unit.

11.3.2 Criteria

Depending upon the size and organisational structure of the firm the same person may operate as both the MLCO and the MLRO. In the case of a sole practitioner, the owner adopts, by default, the role of both MLCO and MLRO.

The Commission issued guidance notes in May 2013 with regard to the appointment of the Money Laundering Reporting Officer and Money Laundering Compliance Officer. However at this early stage of supervision by the Commission the strict criterion for acceptance as MLRO and MLCO is not followed in its entirety.

The important factor is the nomination of an individual(s) who will then be expected to take advantage of any available training provided by the Commission, as well as making their own arrangements to up-skill the individual, by means of the various sources of professional qualification.

11.3.2.1 Positioning the MLCO and MLRO within the organisational structure.

The appointed person must possess sufficient independence to perform the role objectively having unfettered access to all business lines, support departments and information necessary.

Firms must assess and implement their own approach to the two roles of MLCO and MLRO, within the existing organisational structure and the level of AML/PTF risk assessed.

Organisational matters to be considered are such that the MLRO/MLCO must have;

- Sufficient resources including sufficient time.
- A sufficient level of authority within the business.
- Regular contact with the Board or senior management.
- Sufficient knowledge and experience in AML and PTF matters
- Local residency and be employed by the business.

11.4 Outsourcing

Depending upon the nature and the size of the firm the roles of the MLCO and the MLRO may require additional support and resources. Where an accountant selects to bring in additional support or to delegate areas of the MLCO or MLRO functions to third parties, the MLCO and MLRO shall remain directly responsible for their respective roles, and senior management will remain responsible for overall compliance with the money laundering regulations and by extension the Guidance Notes.

The methodology and approach to risk assessment is the decision of the individual firms and is dependent on the nature of the firm and its business.

Any arrangement to outsource its compliance function must have the prior approval of the Commission and be covered by way of a contractual agreement in which defined responsibilities must be clearly sated and acknowledged by all parties.

12 Client Due Diligence (CDD)[11]

12.1 Introduction

Part III of the Code provides extensive detail on the requirements of Client Due Diligence.

12.2 Risk Approach to Client Due Diligence

Using the risk characteristics identified following the business lever risk assessment, client on boarding should include a risk assessment of each client. Businesses are expected to assess the inherent AML and PTF risk associated with each individual new client and also re-assess that risk periodically.

12.2.1 Client Profile

It is necessary to prepare a profile on each client on the basis of CDD information obtained, expected activity and transactions.

The client profile must contain sufficient information to identify:

- CDD information.
  - Identity information and verification.
  - A pattern of expected business activity and transactions within each client relationship; and
  - Unusual, complex or higher risk activity and transactions that may indicate money laundering or terrorist financing activity.

The client level risk assessment may be developed upon a series of characteristics**.** In conjunction with the Business Risk Assessment findings, listed below are a series of characteristics which businesses may wish to use in developing a client risk profile.

12.3 Client Risk

[11] Part III of the Code

Determining the potential money laundering or terrorist financing risk posed by a client or category of clients is critical to the development and implementation of an overall risk based framework. Based upon its own criteria an accountant should seek to determine whether a particular client poses and higher risk and the potential impact on that assessment.

- Transparency of applicant or client. For example, persons that are subject to public disclosure rules, e.g. on exchanges or regulated markets (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, may indicate lower risk.
- Clients where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owners and controllers may indicate higher risk;
- Secretive clients. Whilst face to face contact with clients is not always necessary or possible, an excessively obstructive or secretive client may be a cause for concern;
- Reputation of applicant or client. For example, a well-known, reputable person, with a long history in its industry, and with abundant independent information about it and its beneficial owners and controllers may indicate lower risk;
- Behaviour of applicant or client. For example, where there is no commercial rationale for the service that is being sought, or where undue levels of secrecy are requested, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered, may indicate higher risk;
- The regularity or duration of the relationship. For example, longstanding relationships involving frequent client contact that result in a high level of understanding of the client relationship may indicate lower risk;
- Value of assets or scale and size of transactions.
- Delegation of authority by the applicant or client. For example, the use of powers of attorney, mixed boards and representative offices may indicate higher risk;

12.4 Geographical Risk

Money laundering and terrorist financing risks have the potential to arise from almost any source, such as the domicile of the client, the location of the transaction and the source of the funding. Countries that pose a higher risk include;

- Residence in, or connection with, higher risk jurisdictions.
    - those that are generally considered to be un-cooperative in the fight against money laundering and terrorist financing;
    - those that have inadequate safeguards in place against money laundering or terrorism;
    - those that have high levels of organised crime;
- Those countries that have strong links (such as funding or other support) with terrorist activities;
    - those that are vulnerable to corruption; and
    - those that are the subject of United Nations ("UN"), EU or OFAC sanctions measures.
- Geographical sphere of business activities, e.g. the location of the markets in which a client does business.
- Familiarity with a country, including knowledge of its local legislation, regulations and rules, as well as the structure and extent of regulatory oversight, for example, as a result of a firm's own operations within that country.

12.5 Service Risk

A client risk assessment should also include determining the potential risks presented by the services offered to the client and the ease by which they could gravitate to other services. The context of the services being offered or delivered is always fundamental to a risk based approach.

Any one of the factors considered below may not in itself constitute a high risk circumstance. High risk circumstances can be determined only by the careful evaluation of a range of factors, that cumulatively and after taking into account any mitigating circumstances would warrant increased risk assessment.

- Instructions that are unusual in themselves or that are unusual for the firm or the client may give risk to concern, particularly where no rational or logical explanation can be given.

- Taking on work which is outside the firm's normal range of expertise can present additional risks because money launderer might be using the firm to avoid answering too many questions.
- Accountants should be wary of niche areas of work in which the firm has no background, but in which the client claims to be an expert.
- If the client is based outside the Turks and Caicos Islands, consider why there is such an instruction. For example, have the firm's services been recommended by another client?
- Firms should be wary of:
    - loss making transactions where the loss is avoidable;
    - dealing with property where there are suspicions that it is being transferred to avoid the attention of either a trust in a bankruptcy case, a revenue authority, or a law enforcement agency; or
    - settlements which are intended to be paid in cash, particularly where cash is to be passed directly between sellers and buyers without adequate explanation.

12.6 Ascertain Client Identity – Know your Client[12]

12.6.1 Overview

The general principle is that an accountant must establish satisfactorily that he is dealing with a real person or organization (not fictitious) and obtain identification evidence sufficient to establish that the client is that person or organization. In the case of an organization, it must be ascertained that the client is duly authorized to act for the organization.

Identity information must be verified by reference to independent and reliable source material. The Code Section III provides full details of the approach to verification of client information.

[12] Part III of the Code

If a prospective cannot satisfactorily satisfy usual due diligence measures for example unable to identify and verify a client's identity or obtain sufficient information about the nature and purpose of a transaction, then the transaction must not be carried out the business relationship must not be established.

Firms must also consider submitting a Suspicious Activity Report to the Financial Intelligence Unit.

12.7 Source of Funds

The source of funds for each applicant client must be established.

Source of funds is regarded as the activity which generates the funds for a relationship e.g. a client's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant.

This Guidance stipulates record keeping requirements for transaction records which require information concerning the remittance of funds also to be recorded (e.g. the name of the bank and the name and account number of the account from which the funds were remitted). This is the source of transfer and must not be confused with source of funds.

12.8 Source of Wealth

Source of wealth is distinct from source of funds, and describes the activities which have generated the total net worth of a person both within and outside of a relationship, i.e. those activities which have generated a client's funds and property. Information concerning the geographical sphere of the activities that have generated a client's wealth may also be relevant. In determining source of wealth it will often not be necessary to establish the monetary value of an individual's net worth.

12.9 Is the client acting for a third party?[13]

[13] See Glossary; Beneficial Owner

Reasonable measures must be taken to determine whether the client is acting on behalf of a third party.

Such cases will include where the client is an agent of the third party who is the beneficiary and who is providing the funds for the transaction. In cases where a third party is involved, information on the identity of the third party and their relationship with the client must be obtained.

In deciding who the beneficial owner is in relation to a client who is not a private individual, (e.g., a company or trust) it is essential to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support.

Reference should be made to the Code for further information on the concept of beneficial ownership.

Particular care should be taken to verify the legal existence and trading or economic purpose of corporates and to ensure that any person purporting to act on behalf of the company is fully authorized to do so.

12.10 High Risk Client/ Transactions[14]

There are clients and types of transactions, services and products which may pose higher risk to a business.

Where a relationship or transaction is assessed as presenting a higher risk, firms must perform appropriate Enhanced Due Diligence. (EDD)

Where a relationship or transaction involves a Politically Exposed Person (PEP) then it must always be considered to present a higher risk.

A firm must apply one or more enhanced due diligence measures with higher risk client relationships. The nature of the measures to be applied will depend on the circumstances of the relationship or transactions and the factors leading to the relationship being considered as higher risk.

[14] Section IV of the Code

Enhanced due diligence measures include:

- Requiring higher levels of management approval for higher risk new client relationships.
- Obtaining further Client Due Diligence (CDD) information (identification information and relationship information, including further information on the source of funds and source of wealth), from client or independent sources, such as the internet, public and commercially available databases.)
- Taking additional steps to verify the CDD information obtained.
- Commissioning due diligence reports from independents experts to confirm the veracity of CDD information held.
- Requiring more frequent review of client relationships.
- Requiring the review of client relationship to be undertaken by the compliance function, or other employees not directly involved in managing the client relationship; and
- Setting lower monitoring thresholds for transactions connected with the client relationship.

12.11 Politically Exposed Persons (PEPs)

Corruption by some high profile individuals, generally referred to as PEPs inevitably involves serious crime, such as theft or fraud and is of global concern. The proceeds of such corruption are often transferred to other jurisdictions and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates.

By their very nature, money laundering investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both businesses and jurisdictions concerned, in addition to the possibility of criminal charges.

Indications that an applicant or client may be connected with corruption include excessive revenue from “commissions” or “consultancy fees” or involvement in contracts at inflated prices, where unexplained “commissions” or other charges are paid to third parties.

The risk of handling the proceeds of corruption, or becoming engaged in an arrangement that is designed to facilitate corruption is greatly increased when the arrangement involves PEP. Where the PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

PEP status itself does not of course, incriminate individuals or entities. It will however put an applicant for business or client into a higher risk category.

13 Monitoring Client Activity[15]

13.1 Introduction

Firms must as part of its on-going client due diligence procedures establish appropriate client activity and transaction monitoring procedures so that money laundering monitor client relationships and put in place procedures to identify and scrutinise complex, unusual higher risk activity or where there is no apparent economic or visible lawful purpose.

A risk assessment and development of the client profile will provide knowledge of expected activity. This will provide a basis for recognising unusual and higher risk activity or transactions which may indicate money laundering or terrorist financing. Additional or more frequent monitoring is required for relationships that have been designated higher risk.

13.2 Approach to Monitoring

For the purposes of this section "monitoring" does not oblige the accountant to function as, or assume the role of, a law enforcement or investigative authority vis-a-vis his or her client. It rather refers to maintaining awareness throughout the course of work for a client to money laundering or terrorist financing activity and/or changing risk factors.

The more a firm knows about its clients and develops an understanding of the instructions, the better placed it will be to assess risks.

[15] Part IV Section 28 of the AML Code

In determining the nature of the monitoring procedures that are appropriate an Accountant may have regard to the following factors.

- Its business risk assessment
- The size and complexity of the business
- The nature of its services
- Where it is possible to establish appropriate standardised parameters by unusual activity and
- The monitoring procedures that already exist to satisfy other business needs.

An effective monitoring system requires firms to maintain up to date CDD information and to ask pertinent questions to determine whether there is a rational explanation for the activity or transactions identified. The scrutiny of activity and transactions may involve requesting additional CDD information.

Monitoring may involve real time and post event monitoring, and is likely to be most effective when undertaken on a case by case basis by fee earners, administration and accounts staff.

Sufficient guidance and training of fee earners, account and administration staff is essential to enable them to recognise money laundering and terrorist financing activity.

Firms should also assess the adequacy of any systems, controls and processes on a periodic basis. Monitoring programs can fall within the system and control framework developed to manage the risk of the firm. The results of the monitoring should also be documented.

13.3 Identifying unusual activity/transactions

Appropriate factors to consider in determining whether activity or transactions are unusual include:

- The expected frequency, size, and origin/destination of client funds or other activity for individual clients; and
- The presence of risk factors specific to the nature of the activity or matter undertaken for the client. A firm should determine risk factors based on its knowledge of its client and

should have regard to typologies (whether from its own experience or from external sources) relevant to the nature of its business activities.

13.4 Examining unusual activity.

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

Appropriate action may include

- Making further enquiries to obtain any further information required to enable a determination as to whether the activity/transaction has a rational explanation and
- Considering the activity or transaction in the context of any other relationship connected with the client.
- Updating CDD information to record the results of the enquiries made
- Reviewing the appropriateness of the client risk assessment in light of the unusual activity and/or additional CDD information obtained.
- Applying increased levels of monitoring to particular relationships.
- Where the activity or transaction does not have a rational explanation considering whether the circumstances require a suspicious activity report.

14 Reporting Suspicious Activity and Transactions[16]

14.1 Overview

Section 120 (1) of The POCO calls for:

Where a person

a) knows or suspects or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and

[16] Part V of the AML Code

b) 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 relevant business;

he shall disclose the information or other matter as soon as is practicable after it comes to him to the relevant Money Laundering Reporting Officer or to the Reporting Authority.

In the Turks and Caicos Islands the reporting authority is the Turks and Caicos Islands Financial Intelligence Unit. (FIU).

14.2 What constitutes knowledge or suspicion

14.2.1 Knowledge

Knowledge means actual knowledge.

14.2.2 Suspicion

The test for whether a person holds a suspicion is a subjective one. If someone thinks a transaction is suspicious they are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. They may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. There does not have to be evidence that money laundering is taking place for there to be a suspicion.

If someone has not yet formed a suspicion, but they have cause for concern, a firm may choose to ask the client or others more questions. The choice depends upon what is already known, and how easy it is to make enquiries.

14.2.3 Reasonable Grounds to Suspect

A person would commit an offence even if they did not know that or suspect that a money laundering offence was being committed, if they had reasonable grounds for knowing or suspecting that it was.

If there are factual circumstances from which an honest and reasonable person, engaged in a similar business, should have inferred knowledge or formed the suspicion that another was engaged in money laundering or that there was knowledge of circumstances which would put a reasonable person to enquiry.

It is important that accountants and their staff do not turn a blind eye to information that comes to their attention. Reasonable enquiries should be made, such as a professional in that profession would, based upon their qualifications, experience and expertise might be expected to make in such a situation within the normal scope of their client relationship.

Exercising a healthy level of professional scepticism should be adopted. If in doubt a professional should exercise a level of caution and report to the firms MLRO.

14.3 Failure to report

Failing to report to the FIU knowledge or suspicion of crime proceeds or terrorist property is a criminal offence. If such a transaction is allowed to continue despite there being reasonable grounds to believe that the funds are criminal proceeds or terrorists' funds and a report is not submitted to the FIU then an offence of money laundering or financing of terrorism may have been committed.

14.4 Reporting Procedures

It is the responsibility of the Money Laundering Reporting Officer to submit Suspicious Activity Reports to the FIU.

The relationship between reporting entities and the FIU is a key one, because the FIU can only perform its analytical function to produce financial intelligence if the various reporting entities report the critical information they have.

14.4.1 Internal Reporting Procedures

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

- The circumstances in which a disclosure is likely to be required
- How and when information is to be provided to the MLRO
- Resources which can be used to resolve difficult issues around making a disclosure
- How and when a disclosure is made to the FIU
- How to manage a client when a disclosure while waiting for consent and
- The need to be alert to tipping off issues.

Once employees have reported their suspicions under internal procedures to the MLRO, they have fully satisfied their statutory obligations.

14.5 Evaluation of SARS by MLRO

In order to demonstrate that a report is considered in light of all relevant information when evaluating a suspicious activity report, the MLRO may:

- Review and consider transaction patterns and volumes, previous patterns of instructions, the length of the business relationship and CDD information; and

- Examine other connected accounts or relationships. Connectivity can arise through commercial connections, such as transactions to or from other clients or common introducers, or through connected individuals, such as third parties, common ownership of entities or common signatories.

However, the need to search for information concerning connected accounts or relationships should not delay the making of a report to the FIU.

14.6 Reports to Reporting Authority (FIU)

The MLRO will submit suspicious activity reports to the FIU in writing on the Suspicious Activity Report form electronically via email or they may be delivered by hand. A copy of the SAR form is available via the FIU link on the following website: www.tcipolice.tc or they can be provided by contacting the FIU directly at 649-941-7690 or fcutcipd@tciway.tc

A SAR must be made as soon as it is reasonably practicable to do so once knowledge or suspicion, or reasonable grounds to know or suspect, has been formulated. As such it must be made either before a transaction occurs, or afterwards, if knowledge or suspicion is formulated with the benefit of hindsight after a transaction or activity occurs.

Firms should keep comprehensive records of suspicions and disclosures because disclosure of a suspicious activity or transaction is a defence to criminal proceedings. Such records may include notes which contain:

- on-going monitoring undertaken and concerns raised by fee earners and staff;
- discussions with the MLRO regarding concerns;
- advice sought and received regarding concerns;
- why the concerns did not amount to a suspicion and a disclosure was not made;
- copies of any disclosures made;
- conversations with FIU, insurers, supervisory authorities etc. regarding disclosures made; and
- decisions not to make a report to FIU which may be important for the MLRO to justify his position to law enforcement.

14.7 Tipping Off

When a Suspicious Activity Report has been submitted to the FIU, the accountant or any member of staff must not disclose that such a Report or the content of such Report to any person including the client. It is an offence to deliberately tell any person, including the client, that the business has filed a suspicious transaction report about the client's activities/transactions.

14.7.1 Normal Enquiries

There is nothing in the legislation which prevents a firm from making normal enquiries about a client instructions, and the proposed retainer, in order to remove, if possible any concerns and enable a firm to decide whether there is a suspicion. Firms may also need to raise questions during a retainer to clarify such issues.

It is not tipping-off to include a paragraph about a firm's obligations under the money laundering legislation in a firm's standard client care letter.

In circumstances where a SAR has been filed with the FIU, but CDD procedures are incomplete, the risk of tipping-off a client (and its advisers) may be minimised by: ensuring that employees undertaking due diligence enquiries are aware of tipping-off provisions and are provided with adequate support, such as specific training or assistance from the MLRO; obtaining advice from the FIU where a financial services business is concerned that undertaking any additional due diligence enquiries will lead to the client being tipped-off; and obtaining advice from the FIU when contemplating whether or not to ask for non-routine information or questions in relation to such clients.

14.8 Consent to Activity

14.8.1 Pre-transaction consent[17]

When a SAR is made before a suspected transaction or event takes place FIU consent must be obtained before the event occurs. Consent will only be given in respect of that particular transaction or activity and future transactions or activity should continue to be monitored and reported as appropriate.

[17] Section 116 of The POCO

In the vast majority of instances in which a SAR for consent is made to the FIU, consent to continue an activity or to process a suspected transaction will be provided within seven days of receipt of a report. Whilst this is what generally occurs in practice, the FIU is not obliged under the legislation to provide consent within a particular timeframe, or at all. In particular, consent may be delayed where information is required by the FIU from an overseas financial intelligence unit.

14.9 Terminating the relationship

A firm is not obliged to continue relationships with clients if such would place them at commercial risk. However, to avoid prejudicing an investigation, the FIU may request that a relationship is not terminated.

If a firm, having filed a SAR, wishes to terminate a relationship or transaction, and is concerned that, in doing so, it may prejudice an investigation resulting from the report, it should seek the consent of the FIU to do so. This is to avoid the danger of tipping off.

15 Employee Training and Awareness[18]

15.1 Overview

One of the most important controls over the prevention and detection of money laundering and terrorist financing is to have appropriately vetted staffs that are:

- Alert to money laundering and terrorist financing risks
- Well trained in the identification of unusual or higher risk activities or transactions, which may indicate money laundering or terrorist financing activity.

The effective application of even the best designed control systems can be quickly compromised if staff lacks competence or probity, are unaware of or fail to apply systems and controls and are not adequately trained.

[18] The Code Part VI Section 33

In particular fee earners and those who handle or are responsible for the handling of client transactions will provide the business the business with its strongest defence or weakest link.

A firm should also encourage its fee earners and other staff to "think risk" as they carry out their duties within the legal and regulatory framework governing money laundering and terrorist financing.

15.2 Obligations

Firms must provide their staff with appropriate and proportional training AML/CFT training.[19], There must be a commitment to having appropriate controls relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant firms employees with at least general information on AML/CFT laws, regulations and internal policies. To satisfy a risk-based approach, particular attention should be given to risk factors or circumstances occurring in the Accountants own practice.

Employers are encouraged to produce continuing education programs on AML/CFT and the risk-based approach.

Applying a risk-based approach to the various methods available for training, however gives firms flexibility regarding the frequency, delivery mechanisms and focus of such training. Management should review their own staff and available resources and implement training programs that provide appropriate AML/PTF information that is:

- Tailored to the relevant staff responsibility (*e.g.* client contact or administration). At the appropriate level of detail (*e.g.* considering the nature of services provided by the firm).
    - At a frequency suitable to the risk level of the type of work undertaken by the firm.
    - Used to test to assess staff knowledge of the information provided.

16 Record Keeping[20]

[19] Part VI of the Code
[20] The Code Part VII Sections 34 to 40

The record keeping obligations are essential to facilitate effective investigation, prosecution and confiscation of criminal property.

Records must be kept in a manner which allows for swift reconstruction of individual transactions and provides evidence for prosecution of money laundering and other criminal activities.

Records may be kept in electronic or written form for a period of five (5) years or such longer period as the FSC. The records must be kept for five (5) years after the end of the business relationship or completion of a one-off transaction.

If a business outsources record keeping to a third party, the business remains responsible with the record keeping requirements of the AML/PTF Regulations and the Code.

17 Appendix A Red Flag Indicators

Based upon the analyses of the typologies exercise undertaken by the FATF the following red flags are provided for information. It must be remembered that these are red flags, which should prompt further enquiry and consideration. Appearance does not necessarily indicate money laundering.

This list is not exhaustive and non-appearance of a factor or characteristic on this list does not mean automatically that it is an acceptable situation.

Accountants are encouraged to adopt a healthy level of professional scepticism and to make reasonable enquiries if they come across information which could form the beginning of suspicion.

Accountants are well placed to have a sense of a particular transaction which appears to lack justification or cannot be rationalised as falling within the usual parameters of legitimate business.

17.1 Red Flags about the Client

- Client is uncertain about location of company records
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.

17.2 Red flags relating to the supply of accounting services

- Company records consistently reflect sales at less than cost, thus putting the company into a loss position but the company continues without reasonable explanation of the continued loss.

- Company is invoiced by organisations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven. .
- Client has business activity inconsistent with industry averages or financial ratios.
- Company is paying unusual consultant fees to offshore companies.
- Company shareholder loans are not consistent with business activity.
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.

17.3 Red flags about Source of Funds

- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client appears to be living beyond his or her means.
- Client has numerous accounts and deposits cash into each of them, with the total credit being a large amount.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Client acquires significant assets and liquidates then quickly with no explanation
- Client acquires significant assets and encumbers them with security interests that do not make economic sense
- Clients repays a problem loan unexpectedly
- Loan transactions are entered into in situations where the client has significant assets and the loan transaction does not make economic sense.
- Loans secured by obligations form offshore banks.
- Loans to and from offshore companies

- Transactions involving an offshore shell bank whose name may be very similar to the name of a major legitimate institution.

17.4 Red Flags about the Choice of Auditor

- Use of many different firms of auditors and advisors for connected companies or businesses
- Client has a history of changing bookkeepers or accountants yearly.

18 Glossary

AML/PTF	Anti-Money Laundering and Prevention of Terrorist Financing	Description used in TCI legislation
AML/CTF	Anti-Money Laundering and Combating (or Countering) Terrorist Financing	An alternative shortened form used by other Anti-Money Laundering bodies.
BO	Beneficial Owner	The natural person who ultimately owns or controls the client relationship through which a transaction is being conducted. It also incorporates those persons who exercise ultimate control over a legal person or arrangement.
CDD	Client Due Diligence	Includes not only establishing the identity of clients, but also monitoring activity to identify those transactions that do not conform with the normal or expected transactions for that client or type of account
CFATF	Caribbean Financial Action Task Force	A FATF styled regional body comprising Caribbean states.
DNFBP	Designated Non Financial Businesses and Professions	Within its 2003 revision FATF recommended the inclusion of a series of additional businesses and professions within the scope of the Anti-Money Laundering Regulations.
FATF	Financial Action Task Force	An international policy making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide. Thirty-four countries and two international bodies are members.
FIU	Financial Intelligence Unit.	The Financial Intelligence Unit (FIU) of Turks and Caicos Islands is the Money laundering Reporting Authority (MLRA) which has been established under section 108 of the Proceeds of Crime Ordinance 2007. Authorised to receive Suspicious Activity Reports.
MLCO	Money Laundering Compliance	

	Officer	
MLRO	Money Laundering Reporting Officer	
OFAC	Office of Foreign Assets Control	Office within the U.S. Department of the Treasury that administers and enforces economic and trade sanctions against targeted foreign countries, terrorist-sponsoring organisations, terrorists, international narcotics traffickers, and others based on U.S foreign policy and national security goals.
PEP	Politically Exposed Person	An individual who has been entrusted with prominent public functions in a foreign country, such as head of State, senior political, senior government official, judiciary, or military official, senior executive of a state owned corporation or important political party official, as well as their families and close associates.