

(NBAA)

**THE NATIONAL BOARD OF ACCOUNTANTS AND AUDITORS
TANZANIA**

**ANTI-MONEY LAUNDERING GUIDELINES FOR ACCOUNTANTS
AND AUDITORS (REVISED 2025)**

Table of Contents

ACRONYMS.....	i
PREFACE.....	ii
1.0 INTRODUCTION	1
1.1 Preamble	1
1.2. Objectives.....	5
1.3. Legal basis of the guidelines	5
1.4. Scope and applicability of the guidelines	6
2.0 THE OFFENCES UNDER AML/CFT REGIME	6
2.1. Money Laundering Offence.....	6
2.2. Terrorist Financing Offences	7
2.3. Proliferation Financing Offences.....	7
2.4. Tipping Off.....	8
2.5. Failure to comply with AML/CFT provisions	8
3.0. PROFESSIONAL OBLIGATION.....	8
4.0. AML/CFT SYSTEMS AND CONTROLS.....	9
5.0. RISK BASED APPROACH.....	10
6.0. CUSTOMER DUE DELIGENCE (CDD)	12
6.1. Simplified Due Diligence	13
6.2. Customer Due Diligence	13
6.3. Enhanced Due Diligence	14
6.4 Reliance on Third Party Customer Due Diligence.....	15
7.0 RECORD KEEPING	16
8.0 REPORTING OBLIGATIONS	16
8.1 Proliferation Financing	16
8.2 Suspicious Transaction Reports.....	17
8.2 Cash/Currency Transaction Reports	18
8.3 Terrorist Property Reports	18
8.4 Post Report Action.....	19
9.0 INTERNAL REPORTING PROCEDURES	19
10. TERRORIST FINANCING SANCTIONS	20
10.1 Protection from Liability.....	20
11.0 STAFF TRAINING AND TRAINING PROGRAMMES	22
ANNEXURE: CASE STUDIES	23

ACRONYMS

AMLA	Anti-Money Laundering Act, 2006 (Cap. 423)
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
AMLR	Anti-Money Laundering Regulations, 2012
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
EDD	Enhanced Due Diligence
EOCCA	The Economic and Organised Crime Control Act
FIU	Financial Intelligence Unit
IFAC	International Federation of Accountants
ISA	International Standards on Auditing issued by the International Auditing and Assurance Board (IAASB)
KYC	Know Your Client
NBAA	National Board of Accountants and Auditors
NOCLAR	Non-compliance with Laws and Regulations
MLRO	Money Laundering Reporting Officer
PEP	Political Exposed Person
POCA	The Proceeds of Crime Act, 1991
POTA	The Prevention of Terrorism Act, CAP
19. STR	Suspicious Transactions Register
TPF	Tanzania Police Force
UN	United Nations
URT	United Republic of Tanzania
WMD	Weapon of Mass Destruction

PREFACE

The National Board of Accountants and Auditors (NBAA) has a duty to make sure that its members throughout the country comply with relevant laws, regulations and guidelines. NBAA for the first time in January 2010, issued the Anti-Money Laundering Guidelines for Accountants and Auditors in collaboration with Financial Intelligence Unit (FIU) to assist its members to comply with the requirements of the Anti-Money Laundering Act (AMLA), CAP. 423 and its regulations.

The NBAA in conformity with time-to-time changes of AML/CFT legislations has seen the need to revise the above said Guidelines so as effectively to assist members to implement their legal obligations.

Accountants and auditors being reporting persons under Section 3 of the AMLA are obliged to carry out customer due diligence, maintain records, report suspicious transactions and maintain internal reporting procedures aimed to detect and prevent money laundering and financing of terrorism (ML/TF) activities. In addition, they are required to facilitate the investigation and prosecution of money laundering and terrorist financing offences.

The revised Guidelines provide members with more details on the requirements of the Prevention of Terrorism Act (POTA), CAP 19, Cash Transaction Report Regulations and considerations of the National ML/TF Risk Assessment conducted in 2016, which encourage the application of risk-based approach.

The revised Guidelines have included case studies on fighting money laundering, terrorist financing and economic crime in order to provide some practical guidance to members and the lesson to be learned from those case studies. The case studies have been used only for the purpose of illustrating red flags which members should pick up to identify suspicious activity.

The NBAA appeals to all members of the Accountancy Profession to regularly read and comply with the procedures provided in these guidelines. It is personal responsibility for Accountants and Auditors to observe regulatory framework of AML/CFT regime at several points in the whole process of professional practicing when dealing with individual, entity or third party.

The Guideline is also freely available for download from the Board's website www.nbaa.go.tz

CPA Pius A. Maneno

EXECUTIVE DIRECTOR

1.0 INTRODUCTION

1.1 Preamble

The legal system regulating the Anti-money Laundering (AML) and Counter Financing of Terrorism (CFT) in United Republic of Tanzania (URT) make it mandatory for accountants and auditors to perform their obligations in the detection and prevention of money laundering and terrorist financing transactions. In so doing accountants and auditors being NBAA regulated entities and individuals are required to facilitate the preventive measures, investigation and prosecution of money laundering, terrorist financing and proliferation financing offences.

The legal system regulating the Anti-money Laundering (AML), Counter Financing of Terrorism (CFT) and Countering Proliferation Financing (CPF) in United Republic of Tanzania (URT) consist of: the Proceeds of Crime Act No 25 of 1991; the Economic and Organized Crime Control Act, Cap 200; the Prevention and Combating of Corruption Act, Cap 329, R.E 2022; the Tax Administration Act, Cap 438, R.E 2019 and the Anti-money Laundering Act, CAP 423, 2006 [For Tanzania Mainland]. For the Tanzania Zanzibar include Anti-money Laundering and Proceeds of Crime Act, 2010; Zanzibar Anti-corruption and Economic Crimes Act No. 5 of 2023 and the Zanzibar Drugs Control and Enforcement Authority Act, 8/2021 to mention the few. The National Defense Council Act 2010, and the Prevention of Terrorism Act of 2002 applies throughout the URT (Mainland and Zanzibar).

The legal system in United Republic of Tanzania reveals the government commitment in complying with international instruments in fighting Money Laundering, Financing of Terrorism and Proliferation Financing. The international instruments regulating the fight against Money Laundering and Financing of Terrorism includes: The Charter of the United Nations 1945; The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 [The Vienna Convention]; the United Nations Convention against Transnational Organized Crime, 2000 [The Palermo Convention], the International Convention on Suppression of Financing of Terrorism 1999; Resolution 1373 (2001) adopted by the security council in November 2001, and Resolution 1377 (2001) adopted by the security council in September 2001 to mention the few.

In view of the above, the National Board of Accountants and Auditors (NBAA) issued anti-money laundering guidelines for accountants and auditors in 2010 and revised it in 2019. Due to changes of AML/CFT legislations from time to time, it has been necessary to review and update the said guidelines to accommodate the changes.

The National Board of Accountants and Auditors (NBAA) has reviewed these guidelines in consultation with the Financial Intelligence Unit (FIU) and the Tanzania Police Force (TPF) to provide guidance to accountants, auditors, accounting and auditing firms to comply with AML/CFT regime. Accountants, auditors, accounting and auditing firms are reminded that the ultimate responsibility and accountability for ensuring compliance with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws, regulations and guidelines rests with themselves as they are covered by the AMLA as reporting persons.

The expressions used in this Guideline shall, except where expressly defined in the Guideline or where the context otherwise requires, have the same respective meanings as in the AML/CFT legislations.

AML/CFT Institutional Setup

In implementing AML/CFT regime, the legal system in United Republic of Tanzania designates various institutions with varied responsibilities namely: the Minister Responsible for Finance; The Minister Responsible for Home Affairs; The National Multi-Disciplinary Committee [National Committee]; the Défense Forces Committee; the National Counter Terrorism Centre [NCTC]; the Financial Intelligence Unit [FIU]; Regulators [NBAA being among], Law Enforcement Agencies [Mainland Tanzania]; Law Enforcement Agencies [Zanzibar]; and Reporting Persons.

The Minister Responsible for Finance

The Minister is a senior public official [cabinet member] whom the law confers power on him to: appoint members of the National Committee [See: Sec 8(4) (a) & (b) AMLA]; make regulations for the better carrying out of the purposes and provisions of AMLA [See: Sec 29 AMLA]. specify [by notice], any other person to be a reporting person [See: Sec 3r(j) AMLA]; and specify [by notice] any other regulatory authorities or agencies to be regulatory authorities or agencies [See: Sec 3r(r) AMLA] to mention the few.

The Minister Responsible for Home Affairs

The minister is a senior public official [cabinet member] whom the law confers power on him to: declare any person or organization to be a prescribed Organization if that person or organization meets the criteria for such declaration [See: Sec 6 (1) (a), (b) & (c) POTA]; declare any person a designated party after being satisfied on reasonable grounds that a party has met any of the designation criteria [See: Reg 3m, 5 and 9]; declare any person to be a terrorist [See: Sec 12(1) POTA]; [by order], and treat the counter terrorism convention, as an extradition arrangement between the GURT and another state where the URT is a party to a such counter terrorism convention and there is no extradition arrangement between the URT and another state which is a party to that counter terrorism convention [See: Sec 38(2) POTA].

In addition, the minister responsible for Home affairs is a senior public official [cabinet member] whom the law confers power on him to: make an order requiring a person to leave the URT and remain thereafter out of URT where on reasonable grounds believe that such a person has been, is or will be, involved in the commission of a terrorist act [See: Sec 46(2) POTA]; having regard to the interests of national security and public safety, refuse an application of any person applying for status as a refugee if he or she on reasonable grounds believe that, the applicant has committed a terrorist act or is or is likely to be, involved in the commission of a terrorist act [See: Sec 47 POTA].

The National Multi-Disciplinary Committee [National Committee]

The Committee formulate, assess, regularly review and improve the effectiveness of the policies and measures to combat money laundering and associated predicate offences, terrorist financing and proliferation financing; and advise the Government on legislative, regulatory and policy reforms in respect of anti-money laundering, countering terrorist financing, countering proliferation financing and combating crimes.

Other duties and functions of the committee includes: coordinating activities to identify, assess and create understanding of money laundering, terrorist financing and proliferation financing risks at the national, sectoral, institutional and individual level, to recommend risk mitigation measures, to oversee implementation of the risk assessment action plans and to ensure that such risk assessments are kept up-to-date [Risk Assessment]; and coordinating engagements and engage with regional and international anti-money laundering, countering terrorist financing and countering proliferation financing bodies and advise the Government accordingly, to mention the few.

Defense Forces Committee

The Committee is responsible for conducting the screening for domestic designation or delisting of a party basing on designation or delisting criteria. The committee is established under Regulation 12 of the National Security Council Regulations, 2013. The committee analyses information received from any person, regarding funds or other assets that have been frozen. The committee is being assisted by a secretariat [See: Regulation 3 & 6 POTA].

National Counter Terrorism Centre [NCTC];

National Counter Terrorism Centre is a public institution established within the Ministry of Home Affairs. Under Regulation 8, the National Counter Terrorism Centre is the Secretariat to the Defense Forces Committee and it assist the Committee in the performance of its functions [Regulation 3n].

Financial Intelligence Unit [FIU];

FIU is a public institution within the ministry of finance responsible for receiving, analysing and disseminating suspicious transaction reports, currency transaction reports, cross border currency reports, and electronic funds transfer reports; FIU is responsible for receiving, analysing and disseminating other information regarding actual or potential money laundering, terrorist financing or proliferation financing received from the reporting persons and other sources from within and outside the United Republic [See: Reg. 3f & 4 POTA and Section 4 AMLA].

An institution conferred with an obligation to circulate all designations, any sanctions list or other similar list to Competent Authorities for they have a [regulatory] responsibility to preform [See: Reg. 4(3) (a)]; circulate all designations, any sanctions list or other similar list to the National Security Organs specified in the Constitution for they have a responsibility to preform [See: Reg. 4(3) (b)]; circulate all designations, any sanctions list or other similar list to any other person having a responsibility to detect, freeze or seize the funds or the property of a designated entity under any written law [Reg.4(3) (c) (i)]; and circulate all designations, any sanctions list or other similar list to any other person having a responsibility to take such action as may be necessary to give effect to Resolution 1267, 1373, 1718, 1988 or such other relevant United Nations Security Council Resolution [Reg.4(3) (c) (ii)].

Law Enforcement Agencies [Mainland Tanzania];

Law Enforcement Agencies are state organs and authorities conferred with power to deal with criminal investigations in United Republic of Tanzania. Section 3 of AMLA provides for the list of law enforcement agencies for the purpose of implementation of the Anti-Money Laundering Act in Mainland i.e. Tanzania Police Force, Prevention and Combating of Corruption Bureau, Immigration Services, Tanzania Revenue Authority and other body dealing with criminal investigations.

Law Enforcement Agencies [Zanzibar];

Section 2 of AMLPOCA provides for the list of law enforcement agencies for the purpose of implementation of the Anti-Money Laundering and proceed of Crime Act in Zanzibar, say Tanzania Police Force; Immigration Services; Tanzania Revenue Authority; Zanzibar Revenue Board; and other investigative agency authorized to perform investigation of money laundering or terrorism financing.

Regulators:

The legal system in United Republic of Tanzania does not provide for the definition of a regulator, [but] it rather provides for the obligation and list of institutions designated as regulators [NBAA being among]. These are institutions conferred with an obligation to: enforce compliance by reporting persons in accordance with the AML/CFT requirements [See: Section 23A (1) (a) AMLA]; (b) conduct onsite and offsite examinations for the purpose of monitoring and ensuring compliance by reporting persons [See: Section 23A (1) (b) AMLA]; and (c) impose administrative sanctions for noncompliance [See: Section 23A (1) (c) AMLA].

In addition, Where any reporting person fails to comply with the AML/CFT requirements, the law confers regulators with power to impose: warning or caution not to repeat the conduct which led to non-compliance [See: Section 19A (a) AMLA]; reprimand [See: Section 19A (b) AMLA]; directives to take remedial action or to make specific arrangement to remedy the default [See: Section 19A (c) AMLA]; restriction or suspension of certain business activities [See: Section 19A (d) AMLA]; suspending a business license [See: Section 19A (e) AMLA]; or suspension or removal from office any member of staff who caused or failed to comply [See: Section 19A (f) AMLA]

Reporting Persons

The legal system in United Republic of Tanzania does not provide for the definition of reporting person, [but] it rather provides for the obligation and list of reporting persons as follows:

- a) *Banks and financial institutions;*
- b) *Cash dealer;*
- c) *An accountant, real estate agent, auditor, tax adviser, dealer in precious stones work of arts or metals;*
- d) *Trust and company service provider;*
- e) *Motor vehicle dealer;*
- f) *Clearing and forwarding agent;*
- g) *Advocates, notaries and other independent legal professionals “when”:*
- i. *Assisting clients in preparing or executing transactions involving:*
 - The purchase or sale of real property or commercial enterprises;
 - Management of funds, securities or other assets which belong to a client;
 - The opening or management of bank accounts, saving accounts or portfolios

- The organization of contributions required to create, manage or direct corporations or legal entities
 - The creation, management or direction of corporations or legal entities; and
 - The buying or selling of business entities;
- i. Acting on behalf of a client in any financial or real estate transaction;
 - ii. Pension funds managers, securities market intermediaries, financial leasing entities, microfinance service providers except for community microfinance groups classified as Tier 4 in the Microfinance Act and companies and financing housing companies;
 - iii. Auctioneers; and
 - iv. Any other person who the Minister may, by notice published in the Gazette, specify

1.2. Objectives

These guidelines are published/issued to assist accountants, auditors, accounting firms and auditing firms to fulfill their obligations as enshrined in the anti-money laundering and counter financing of terrorism legislations and providing approaches to meeting them. Specifically, these guidelines aim at;

- a) Providing industry specific guidance for the accountancy sector on their legal obligations for measures to combat ML and FT activities
- b) Promoting integrity of accountants and auditors when dealing with AML/CFT issues.
- c) Describing areas that accountants and auditors wittingly or unwittingly could be victim of circumstances when processing transactions in the due course of their profession obligations.
- d) Help accountants increase their awareness of money laundering and terrorist financing (ML/TF) risks and provide prompts on how to comply with AML/CFT requirements.
- e) Providing accountants, auditors, accounting firms and audit firms an understanding on their obligations to report suspicious transactions, keep records, conduct training, perform customer due diligence, conduct and updating risk assessment, and develop documented policies and procedures.
- f) Assisting NBAA being the regulator to implement AML/CFT supervisory functions as provided for under Section 19A and 23A of AMLA Act. of 2022.

1.3. Legal basis of the guidelines

The National Board of Accountants and Auditors (NBAA) is an independent regulatory body for the accountancy professional established under the accountants and Auditors (Registration) Act, 286 [R.E.2021]. Statutory duties and responsibilities of NBAA includes: registration of members, accounting and auditing firms; regulation of the accountancy sector; Development of Accountancy Profession; formulation and setting accounting and auditing standards; and carrying out such other functions after consultation with the Minister.

Considering its inherent supervisory functions, section 3 of the Anti-Money Laundering Act, Cap 423 designates NBAA to be among the regulatory institutions in the United Republic of Tanzania for the purpose of AML/CFT. Section 4(e) of the Accountants and Auditors (Registration) Act, Cap 286 read together with section 6(f), 19A and 23A of the AMLA requires NBAA in consultation with FIU to issue guidelines to reporting persons under its purview in respect of its obligations provided for under the AMLA, and implement other anti-money laundering, countering terrorist financing and countering proliferation financing obligations. Section 3 of the AMLA designates accountants and auditors as reporting persons and they are obliged to comply with AML/CFT requirements.

Being reporting persons or regulated entities and individuals under NBAA, accountants and auditors need guidelines that would assist them in implementing and complying with the AML/CFT requirements. In assisting its members to properly implement the requirements and obligations of AML/CFT regime without compromising the profession standards, NBAA developed its first guidelines in 2010 and reviewed it in 2019 following reforms in the legal system.

1.4. Scope and applicability of the guidelines

These guidelines are developed to guide all accountants, auditors, accounting and auditing firms in Tanzania. The guidelines are designed to reduce the possibility of accountancy profession being used for any purpose connected with any financial related offences including fraud, tax crimes, theft or money laundering; this means that any person registered as an accountant or auditor comes under the ambit of these guidelines. Branches (where applicable), are considered not to be legally distinct from their head office, and are therefore, subject to AML/CFT legislations. A failure for branches to comply with the legal requirements will automatically be considered as a failure of a group to manage AML/CFT risks.

In addition, these guidelines cover individual accountants including internal auditors employed in public and private sectors. However, they can use other AML/CFT guidelines issued by FIU or their respective employers' regulators suitable to their working environment to supplement these guidelines.

2.0 THE OFFENCES UNDER AML/CFT REGIME

Worldwide, money laundering is committed by launderers with intention to conceal property earned from criminal activities. Money laundering, terrorist financing and proliferation financing affect the social, economic, political and cultural development of a society. These guidelines highlight the offences related to money laundering, terrorist financing and proliferation financing to comply with AMLA and POTA provisions to enable proper reporting, maintenance of internal controls and procedures and disclosure of information.

2.1. Money Laundering Offence

Money laundering offences are provided for under section 12 of AMLA, Cap 423, which prescribe circumstances under which an offence may be committed. However, the offence of money laundering is separate, independent and distinct from the crime underlying money laundering offence. A person is considered to have committed money laundering offence if one of the following is exhibited;

- a) Engages, directly or indirectly, in a transaction that involves property that is proceeds of a predicate offence while he knows or ought to know or ought to have known that the property is the proceeds of a predicate offence;
- b) Converts, transfers, transports or transmits property while he knows or ought to know or ought to have known that such property is the proceeds of a predicate offence, for the purposes of concealing, disguising the illicit origin of the property or of assisting any person who is involved in the commission of such offence to evade the legal consequences of his actions;
- c) Conceals, disguises or impedes the establishment of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, while he knows or ought to know or ought to have known that such property is the proceeds of a predicate offence;

- d) Acquires, possesses, uses or administers property, while he knows or ought to know or ought to have known at the time of receipt that such property is the proceeds of a predicate offence; or
- e) Participates in, associates with, conspires to commit, attempts to commit, aids and abets, or facilitates and counsels the commission of any of the acts described in paragraphs (a) to (d) of this section.

2.2. Terrorist Financing Offences

A person is considered to have committed an offence of terrorist financing if he/she engages in:

- a) The provision of finance or economic resources or making available financial or related services to-
 - (i) A terrorist, terrorist group, terrorist entity, terrorist course or a terrorist act;
 - (ii) An individual, a group or entity that is concerned with a terrorist, terrorist group, terrorist entity, terrorist course or a terrorist act;
- b) Conducting a financial transaction or facilitating a financial transaction directly or indirectly, in order to deal with property that is owned or controlled by a terrorist, terrorist group or terrorist entity;
- c) Conducting financial transaction or facilitating a financial transaction directly or indirectly, in order to deal with property on behalf of a terrorist, terrorist group or terrorist entity;
- d) Financing or facilitating travel of any individual or a group of individuals to a country other than their country of residence or nationality in order to participate in a terrorist course, terrorist training or terrorist act, or in order to directly or indirectly conduct, perpetrate, plan or prepare terrorist acts;
- e) Organizing or directing others to commit any of the acts in paragraphs (a), (b), (c) or (d) or participating in any of those acts as an accomplice; or
- (f) an attempt to commit any of the acts in paragraphs (a), (b), (c), (d) or (e);

2.3. Proliferation Financing Offences

The offence of proliferation financing is considered to be committed, if any person, by any means, directly or indirectly;

- (a) Provides or collects funds, technology or services, with an intention or knowledge that the said funds, technology or services may be used, in full or in part, to carry out an act constituting proliferation financing or to any person or jurisdiction or for the benefit of any person designated by the United Nations Security Council; or
- (b) Deals with, enters into or facilitates any transaction or enables the acquisition of a business interest or performs any other act in connection with funds, which such person knows or ought reasonably to have known or suspected to have been acquired, owned, collected, used, possessed or provided for proliferation financing, commits an offence and shall be liable, on conviction, to imprisonment for a term of not less than twenty years.”.

2.4. Tipping Off

It is common practice for accountants and auditors to access information when performing their duties, of which some may contain criminality. Intentionally or unintentionally accountants and auditors may find themselves disclosing that information to unauthorized persons. The AML/CFT regime has put in place restrictions on disclosure of information in the circumstances provided hereunder;

- a) Disclose or warn any person involved in the transaction or to an unauthorised third party, during the establishment or course of customer relationship or when conducting occasional transactions.
- b) Discloses that, a suspicious transaction report may be prepared, or is being prepared or has been sent to the FIU¹; or
- c) Disclose to a suspect or unauthorised third party the information relating to an ongoing or impending investigation or any other law with the intent to interfere or otherwise frustrate the investigation²

2.5. Failure to comply with AML/CFT provisions

AML/CFT regime has put in place the administrative, civil and criminal sanctions for noncompliance with the provisions related to risk assessment, customer due diligence, record keeping, reporting of suspicious transactions and internal reporting procedures.

The anti-money laundering law empowers FIU or regulator to impose administrative sanctions to the reporting persons for the failure to comply with the above requirements. The sanctions are provided under Section 19A of AMLA Cap 423 as follows;

- (a) Warning or caution not to repeat the conduct which led to non– compliance referred to in sub – regulation (1);
- (b) A reprimand;
- (c) Directive to take remedial action or to make specific arrangement to remedy the default;
- (d) Restriction or suspension of certain business activities; (e) suspending a business license; or
- (f) Suspension or removal from office any member of staff who cause or fail to comply.

However, civil and criminal sanctions are prescribed in AMLA, POTA, POCA and EOCCA depending on the nature of the offence committed.

3.0. PROFESSIONAL OBLIGATION

Accountants and auditors hold a particular prominent position in a society. Based on the premise of high ethical practice, entities and the public at large put their trust in these professionals for their honesty, integrity, and in the client secrecy which is normally associated with such relationship. In most cases such trust is justified by the very fact of their solid reputations which may also be the target of money launderers, who will seek to hide behind their reputation and client secrecy, in order to carry out their illicit activities.

¹ Section 20 of AMLA

² Section 31C of POCA

Money launderers are likely to target accountants and auditors in the hope of using their professional status to minimize suspicion. In this regard, accountants and auditors in carrying out their obligations, are required to:

- a) Seek and obtain an understanding of the matter, once becomes aware of information concerning an instance of non-compliance or suspected non-compliance including the nature of the act and the circumstances in which it has occurred or may occur.
- b) Apply knowledge, professional judgment and expertise, but is not expected to have a level of understanding of laws and regulations beyond that which is required for the professional accountant's role within the employing organization.
- c) Note that, any act that constitutes non-compliance is ultimately a matter to be determined by a court or an appropriate administrative body. To avoid tipping off, an accountant or auditor may consult on a confidential basis with others within the employing organization or a professional body, or with legal counsel.
- d) Consider reporting and consulting procedures existing within the organization, if an accountant or auditor identifies or suspects that non-compliance has occurred or may occur, and may perform the following;
 - i) Inform an immediate superior to enable the superior to take appropriate action.
 - ii) If the professional accountant's immediate superior appears to be involved in the matter, shall inform the next higher level of authority within the employing organization
 - iii) In exceptional circumstances, an accountant or auditor may decide that disclosure of the matter to an appropriate authority is an appropriate course of action, if doing so, will not be considered a breach of the duty of confidentiality.
 - iv) When making such disclosure referred in (iii) above, an accountant or auditor shall act in good faith and exercise caution when making statements and assertions

4.0. AML/CFT SYSTEMS AND CONTROLS

Under the AML/CFT regime reporting persons are required to establish appropriate risk-sensitive policies and procedures in order to prevent activities related to ML/TF including those policies, controls and procedures which provide for:

- i) Customer Due Diligence (CDD), i.e., procedures designed to acquire knowledge about the firm's clients, a beneficial owner and prospective clients and to verify their identity as well as monitor business relationships and transactions. Accountants and auditors when conducting CDD should have a risk management system to assist in determining whether a client is a PEP;
- ii) Identification and scrutiny of complex or unusually large transactions, unusual patterns of transactions with no apparent economic or lawful purpose and other activities regarded by the regulated person as likely to be of the nature of money laundering or terrorist financing or proliferation financing;
- iii) Prevention of use of products favoring anonymity;
- iv) Employee are screened and vetted.
- v) Internal reporting procedures clearly put in place including designation of compliance partner and/or appointment of a money laundering reporting officer

(MLRO) from senior management level to receive and access other information related to ML/TF/PF reports required under section 18 of AMLA, Cap 423 and a system for making those reports;

- vi) Record keeping, including details of customer due diligence and supporting evidence for business relationships and records of transactions, which need to be kept for a minimum period of ten years³ ;
- vii) Internal controls, management, compliance monitoring, and communication
- viii) Risk assessment, mitigation measures and allocation of resources,
- ix) Take measures to make relevant employees aware of AML/CFT laws, and to train those employees in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.

In order to ensure compliance is appropriately managed, accountants and auditors will need to ensure sufficient senior management oversight, appropriate analysis and assessment of the risks of clients and product types, effective systems for monitoring compliance with procedures and methods of communicating procedures and other information to personnel.

5.0. RISK BASED APPROACH

Accountants and auditors need to make a reasoned decision as to how they intend to manage money laundering and terrorist financing (ML/TF) risks. A risk-based approach does, however, enable practitioners to target their resources and efforts where the risk is higher and, conversely, reduce requirement where risk is low. In this regard accountant and auditors shall consider⁴;

- a) Risk identification and assessment.

Identification of Money laundering and Terrorist Financing risk facing a firm shall be determined by its threats and vulnerability. When assessing ML and TF threats accountants and auditors shall consider inherent and residual risks factors. In assessing vulnerability, he/she shall consider the nature, size, and complexity of the business; products and services; the jurisdictions of client origin; source of funds; delivery channels, and type and conduct of business.

- b) Risk management and mitigation.

Identify and applying measures to effectively and efficiently mitigate and manage ML/TF risks. This will be classified as High, Medium high, Medium, Medium low and Low. Such an approach is valid, and should be capable of minimizing complexity, but needs to retain an element of discretion and flexibility where risk ratings may be raised or lowered with appropriate management input in response to particular or exceptional circumstances

- c) Ongoing monitoring

Putting in place policies, procedures and information systems to monitor changes to ML/TF risk.

- d) Documentation

Document risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks.

³ Sec 16(1)(b) of AMLA CAP 423

⁴ FATF Accounting profession risk-based approach guidance.

When conducting risk-based assessment for determination of likelihood in terms of threats and vulnerability, require consideration of different types of risk to which they are exposed. For example;

- a). Being used in an active sense to launder money through the handling of cash or assets,
- b). Becoming concerned in an arrangement which facilitates ML/TF, through the provision of investment services or the provision of trust or company services.
- c). Risks attaching to the client and/or those who trade with or otherwise interact with clients as regards their potential for involvement in money laundering.

A simple matrix prepared from a risk-assessment of the factors considered above, may provide a basic framework for the categorization of clients and engagements, and to direct the depth and type of customer due diligence accordingly. Senior management engagement and commitment is needed to produce and embed a successful risk-based approach, and it needs effective communication to all staff members who need to use it.

Developing and applying a risk-based approach

In developing a risk-based approach, accountants and auditors need to ensure it is readily comprehensible and easy to use for all relevant staff. In cases of doubt or complexity, accountants and auditors may wish to consider putting in place procedures where queries may be referred to a senior and experienced person, e.g. the Compliance Partner or MLRO for a risk-based decision, which may vary from standard procedures.

To develop the approach, it is necessary to review the business and consider what ML/TF risks might attach to each service type, client type etc. One-way to consider this in relation to the defined services is outlined below, but there are other approaches that may be equally or more valid depending on the type of business.

Accountants and auditors should consider first the type of risk presented:

- a). Is the risk that the business might be used to launder money or provide the means to launder money? Examples might include handling client money, implementing company and trust structures, handling insolvent estates where assets are tainted by crime etc.
- b). Is the risk that the client or its counterparties might be involved in money laundering? Examples might include clients who are Politically Exposed Persons (PEPs) or who are high profile and attract controversy or adverse comment in the public domain, or who are involved in higher risk sectors and jurisdictions (e.g., those where corruption is known to be a higher risk), or who are known to be potentially involved in illegal activities, such as tax evaders seeking advice to resolve their affairs, and certain forensic work connected with fraud or other crime etc.

Consideration of these risk types should enable the accountants and auditors to draw up a simple matrix of characteristics of the client or service, which are considered to present a higher risk and those, which present a medium risk. Some may, by long acquaintance and detailed knowledge, or by their status qualified for simplified due diligence be considered to present a lower risk.

This matrix can then be incorporated into client acceptance procedures and customer due diligence process that allows a ML/TF risk level to be assigned.

It is important for the approach adopted to incorporate a provision for raising the risk rating from low or medium to high if any information comes to light in conducting the customer due diligence that causes concern or suspicion.

In all cases, even where clients qualify for simplified due diligence or where they are considered low risk for other reasons, to assist in effective ongoing monitoring, accountants and auditors should gather knowledge about the client to allow understanding of:

- (a) Who the client is
- (b) Where required, ultimate beneficial owners
- (c) Who controls it
- (d) The purpose and intended nature of the business relationship
- (e) The nature of the client
- (f) The client's source of funds
- (g) The client's business and economic purpose

The information specified in (a) to (g) above are referred to in the remainder of these guidelines as 'know your client' or 'KYC' information which is one-step in the customer due diligence process. However, accountants and auditors may avail themselves of the opportunity to conduct verification of identity on a simplified basis. Accountants and auditors need to set out clear requirements for collecting KYC information about the client and for conducting verification of identity, to a depth suitable to the assessment of risk.

6.0. CUSTOMER DUE DILIGENCE (CDD)

Customer due diligence measures are an essential part of any system designed to prevent money laundering, terrorist financing and proliferation financing, carried out on risk-sensitive basis. This means that accountants and auditors need to consider how their risk assessment and management procedures flow through into their client acceptance, identification, and verification procedures, to give sufficient information and evidence, in the way most appropriate to the business concerned. Therefore, CDD measures should be carried out:

- a) before establishing a business relationship;
- b) before carrying out an occasional transaction;
- c) where there is a suspicion of money laundering or terrorist financing or proliferation financing;
- d) when the veracity or adequacy of documents, data or information previously obtained for the purposes of customer due diligence is doubted; and
- e) any time after establishing the materiality of money laundering, terrorist financing and proliferation financing risk.

CDD on a risk-based basis include procedures for; simplified due diligence, customer due diligence and enhanced due diligence. However, a professional accountant subject to conditions prescribed in the regulations may rely on third party CDD.

In addition, where accountants or auditors have not been able to associate a particular customer with ML/TF/PF, shall conduct enhanced customer due diligence. The level of identity documentation and verification for each category of CDD shall be in accordance to AML/CFT regulations.

The below summarises requirements of CDD under AMLA regulations.

Regulation 7 – Manner of conducting risk based CDD

Regulation 8 – Customer identification and verification

Regulation 8A- Conducting an on-going monitoring

Regulation 9 – Establishment of internal procedures

Regulation 10 – Application of enhanced due diligence measures.

Regulation 11 – Ending application of simplified due diligence measures.

Regulation 12 – Correspondent banking customer due diligence measures.

Regulation 13 – Reliance on third parties' customer due diligence

Regulation 13A – CDD on branches and subsidiaries.

Accountants and auditors may use various sources of information to enhance business knowledge of their client, including direct discussion with the client. Information sources (*e.g.* websites, brochures, reports etc.) prepared by the client may also help to judge the type of the client. In addition, accountants and auditors may apply independent sources like world check and others to identify high-risk customers such as PEPs, high profile and those listed in the UN, domestic and any other sanction lists. In case of higher risk cases or for high-risk customers, accountants and auditors are required to apply enhanced due diligence. Full details of name and address as well as the details of the identity document provided should also be keenly observed.

If a transaction is being undertaken on behalf of another person, identification evidence of all the persons concerned should be obtained and copies of all documents called for verification should be kept on record. Auditors should make sure that they also adhere to the requirements of International Standards on auditing (ISA 315) – *Obtaining an understanding the entity and its environment and assessing the risk of material misstatements*.

6.1. Simplified Due Diligence

Simplified due diligence are procedures applied to customers that are determined to have ML/TF/PF low risk at the national, sectoral, institutional or individual level risk assessments or based on the relevant information provided by the regulator, FIU or other competent authorities.

Where accountants and auditors believe on reasonable grounds that the clients or services fall under low risk level, may apply simplified due diligence. In any case where a client has been subject to simplified due diligence and a suspicion on ML/TF or predicate offence arises in relation to that client, this type of CDD shall no longer apply.

6.2. Customer Due Diligence

Customer due diligence is the procedure for identification and verification of customer's identity that are associated with ML/TF/PF moderate risk, through personal information and/or entity information from reliable sources

For accountants and auditors, CDD of the business relationship is very important. This comprises scrutiny of activity during the relationship, including enquiry of source of funds if needed, to ensure all is consistent with expected behavior based on accumulated customer due diligence information. He or she when conducting CDD shall also consider the following:

- a) Obtain and verify information on the ultimate beneficial owners of a legal person, entity or arrangement;

- b) In relation to politically exposed person, in addition to undertaking normal due diligence measures-
 - i) Have appropriate risk management systems to determine whether the customer is apolitically exposed person;
 - ii) Obtain senior management approval for establishing business relationship with such customer
 - iii) Take reasonable measures to establish the source of wealth and source of funds; and
 - iv) Conduct enhanced ongoing monitoring on that relationship.

In addition, after conducting CDD a professional accountant shall:

- a) Conduct ongoing monitoring after establishing a business relationship, including the updating of customer information. He/she shall consider updating risk register:
 - i. At the start of new engagements and when planning for recurring engagements.
 - ii. When a previously stalled engagement restart.
 - iii. Whenever there is a change of control and/or ownership of the client. (d) When there is a material change in the level, type or conduct of business; and
 - iv. Where any cause for concern or suspicion has arisen (in such cases, care must be taken to avoid making any disclosure which could constitute tipping off).
- b) Not open or operate an account in a false, disguised, anonymous or fictitious name;
- c) Not commence a business relationship prior to completion of CDD, provided that, under proven low risk, business relationship may commence pending the verification process;
- d) Terminate an existing business relationship when CDD cannot be completed; and
- e) Submit a suspicious transaction report to the FIU when CDD cannot be completed.

It may be helpful for the professional accountant to explain to the client the reason for requiring evidence of identity and disclosure of beneficial owners. This can be achieved by including an additional paragraph in the audit engagement letter. Where client identification procedures start before the engagement letter is drafted, it might be helpful for the professional accountant to address this in pre-engagement letter communications with the potential client.

6.3. Enhanced Due Diligence

Enhanced customer due diligence are procedures applied to customer's identity that are associated with ML/TF/PF high risk. Enhanced due diligence shall be implemented in addition to the general due diligence requirements set out in (6.2) above. It must be applied in the following situations to obtain additional customer due diligence information about the client:

- a) Where there is a high risk of ML/TF/PF;
- b) in any occasional transaction or business relationship with a person established in a high-risk country;
- c) In relation to cross-border correspondent relationships;
- d) If an accountant or auditor has determined that a client or potential client is a PEP, or a family member or known close associate of a PEP;

- e) In any case where a client has provided false or stolen identification documentation, entity registration documents or information on establishing a business relationship;
- f) In any case where a transaction is complex and unusually large, there is an unusual pattern of transactions which have no apparent economic or legal purpose;
- g) In any other case which by its nature can present a higher risk of ML/TF.

The accounting or auditing firm's policy must have internal procedures that set out clearly what should constitute reasonable grounds for a client to qualify for EDD and must take into account at least the high-risk factors. EDD procedures must include:

- a) As far as reasonably possible, examining the background and purpose of the engagement; and
- b) Increasing the degree and nature of monitoring of the *business relationship* in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious.

EDD measures may also include one or more of the following measures:

- a) Seeking additional independent, reliable sources to verify information, including identity information, provided to the *business*;
- b) Taking additional measures to understand better the background, ownership and financial situation of the *client*, and other parties relevant to the *engagement*;
- c) Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the *business relationship*;
- d) Increasing the monitoring of the *business relationship*, including greater scrutiny of transactions.

6.4 Reliance on Third Party Customer Due Diligence.

A professional accountant may rely on CDD conducted by third party on his/her behalf but shall not preclude his/her responsibility according to AML/CFT laws. The following third parties may be relied upon:

- (a) An authorised person;
- (b) A law firm, notary or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction;
- (c) Another reporting person; or
- (d) A member of the reporting person's group.

When a professional accountant has decided to rely on third parties CDD, may only do so if and to the extent that:

- (a) The necessary customer due diligence information is immediately obtained from the third party;
- (b) Adequate steps are taken to satisfy himself that certified copies of the documents used to undertake the relevant elements of CDD will be available from the third party on request without delay;
- (c) Where a third party is in another country, the said third party meets the criteria set out in the AMLR⁵
- (d) Is not in reliance on any exception from the requirement to conduct any relevant elements of CDD which seeks to rely on; and
- (e) The information is up to date

⁵ Regulation 13 of Anti money laundering regulations 2022.

7.0 RECORD KEEPING

A record keeping for AML/CFT is very important for reporting person to track historical records of individuals, entities and transactions. All accountants and auditors are required under section 16 of AMLA read together with regulation 22 of AMLR to establish and maintain records of;

- (a) Client's identity
- (b) The supporting evidence of verification of identity (in each case including the original and any updated records),
- (c) The firm's business relationships with them (i.e. including any non-engagement related documents relating to the client relationship),
- (d) Details of any occasional transactions and details of monitoring of the relationship. Apart from AMLA requirement, NOCLAR guidance require accountants and auditors to document and keep response of management and those charged with governance the courses of action considered, the judgements made, and decisions taken in any issue related to non-compliance with laws and regulations.

These records must be kept for a minimum period of ten years after the end of the relevant business relationships or completion of the transactions. Care is needed to ensure that records retained are retrievable on demand without delay in legible format.

8.0 REPORTING OBLIGATIONS

8.1 Proliferation Financing

"Proliferation financing" literally means an act of providing funds or financial services, which are used for proliferation activities. According to UNSCR 1540 refers to: "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (e.g. Technologies, expertise, software or services) in contravention of existing laws or applicable international obligations".

Taking into account the effect of weapon of mass destruction (WMD) if used by terrorists, the Prevention of Terrorism Act, Cap 19 under section 20, prohibit any person to offer or provide any weapon to any person, member of terrorist group or terrorist group for use of, or benefit of terrorist group or member of terrorist group.

Accountants referred in part II of the schedule of POTA regulations as accountable entity, must comply with the notice issued from the Minister of Home Affairs and implement the following as required by regulations 5(3) and 6(2) if their clients are declared in the list of proscribed terrorist and proliferation criminals, domestically and internationally (UN sanction lists);

- (a) Conduct a check on regular basis to verify whether individuals or entities listed in the notice match with the particulars of their clients and whether they are holding any funds, financial assets or properties of the listed persons or entities;
- (b) Freeze without delay financial assets of such person or organization;
- (c) Conduct ongoing prohibition on the provision of funds and financial assets to the proscribed person or organizations;

- (d) Conduct ongoing review of transactions as they are processed for existing and occasional customers; and
- (e) Inform the Minister of the full particulars of the frozen funds, financial assets or properties.

8.2 Suspicious Transaction Reports

Where the accountant or auditor suspects or has grounds to suspect that, funds or property are proceeds of crime, or are related or linked to or are to be used for commission or continuation of a predicate offence or has knowledge of a fact or an activity that may be an indication of ML/TF/PF or predicate offence, he shall within twenty-four hours after forming that suspicion and, wherever possible, before any transaction is carried out:

- a) Take reasonable measures to ascertain the purpose of;
 - i) The funds or property, transaction or proposed or attempted transaction,
 - ii) The origin and ultimate destination of the funds or property involved, and
 - iii) The identity and address of any ultimate beneficiary;
- b) Prepare a report of the transaction or proposed or attempted transaction and submit the report to FIU.

Where the accountant or auditor knows or suspects, or has reasonable grounds to know or suspect, that another person (client) is engaged in ML/TF/PF or an act constituting a predicate offence, a disclosure must be made to the firm's MLRO who has an obligation to report to the FIU. In doing so the following shall be considered:

- a) Take reasonable measures to ascertain the purpose of;
 - i) The funds or property, transaction or proposed or attempted transaction,
 - ii) The origin and ultimate destination of the funds or property involved, and
 - iii) The identity and address of any ultimate beneficiary;
- b) Prepare a report of the transaction or proposed or attempted transaction and submit the report to FIU.

This applies to both partnership and sole proprietorship firms. The MLRO should have reasonable access to information that may be relevant to determining whether sufficient basis exists, or the suspicion is genuine and hence report to the FIU.

The MLRO is responsible for making decisions on whether the information contained in the suspicious transactions need to be relayed to FIU. The role of the MLRO carries significant responsibility and should be undertaken by a senior person within the accounting and/or auditing firm who has sufficient authority to take independent decisions, and who is properly equipped with sufficient knowledge, and resources, to undertake the role. The key role is that of receiving information on suspicious transactions and reporting to FIU as applicable.

Suspicious transaction report shall be submitted to the FIU as soon as possible but not later than twenty-four (24) hours after an accountant or auditor has become aware or has knowledge of a suspicious transaction (regulation 21 of AMLRs, 2022). The AML legislation also requires accountants and auditors to maintain a suspicious transaction report (STR) register of all reports made to the MLRO.

The register shall contain details of the date on which the report was made, the person who made the report, the amount and the type of currencies involved and any other

information that may have proven or clarify grounds of suspicion⁶. It should also include action taken, i.e. whether the report has been submitted to the FIU or not and the reasons for not submitting.

Reporting to the FIU does not relieve the auditor from other statutory duties. Examples of statutory reporting responsibilities include:

- (a) Auditors of entities in the banking sector have statutory duty to report matters of 'material significance' to the Bank of Tanzania, which come to the auditor's attention in the course of the audit work.
- (b) Auditors of entities in the public sector have statutory duty to report matters of 'material significance' according to the Public Audit Act, 2008 that come to the auditor's attention in the course of the audit work.
- (c) Auditors of other types of entities are also required to report matters of 'material significance' to their respective regulatory authorities.

8.2 Cash/Currency Transaction Reports

Accountants and auditors have obligation to submit cash/currency transaction reports to FIU when such transactions are complex, unusual or large business transactions unusual patterns of transactions and insignificant but periodic transactions, which have no apparent economic or lawful purpose, whether completed or not.

There are circumstances on which accountants and auditors are required to report cash transactions only when they;

- a) Engage in any of the following activities on behalf of any person or entities (client);
 - i. Receiving or paying funds,
 - ii. Purchasing or selling securities, shares, real properties or business assets or entities, or
 - iii. Transferring funds or securities by any means; or
- b) Give instructions on behalf of any person or entity in respect of any activity referred in (a) above.

8.3 Terrorist Property Reports

Accountants and auditors have obligation to disclose to a police officer the existence of any property in their possession or control, which is to their knowledge, owned or controlled by or on behalf of a terrorist group or any information regarding a transaction or proposed transaction in respect of any property⁷.

⁶ Regulation 19 and 20 of AMLR 2022 contains the information that are crucial to determine the credibility of the transactions.

⁷ As per section 41 of POTA, CAP 19

In addition, accountants and auditors shall report without delay⁸ to the FIU any information regarding a transaction or proposed transaction in respect of any property which is to their knowledge, owned or controlled by or on behalf of a terrorist group. Accountants and auditors who have in their possession or under their control a property against which an order of freezing has been issued or granted, shall report the fact of that possession or control in every three months, to the commissioner of FIU⁹.

8.4 Post Report Action.

When an accountant or auditor reports suspicious transaction(s) or any matter related to AML/CFT/CPF to the specific authority, may cautiously continue with the business in compliance with the terms of engagement while avoiding making disclosure that could amount to tipping-off¹⁰.

9.0 INTERNAL REPORTING PROCEDURES

Accounting and auditing firms are required to establish written internal reporting procedures which will assist to:

- a) Ensure proper screening and vetting of new employees.
- b) Designate a natural person as MLRO, to whom all employees shall report any actual or suspicious activities or transactions in terms of ML/TF/PF or any other criminal activity which comes to the attention of employees in the course of work;
- c) Enable the MLRO to have reasonable access to information that may be relevant in determining basis for reporting suspicious activity/transaction to FIU.
- d) Require the MLRO to report the suspicious activity or transaction to the FIU, in the event there exists reasonable grounds to report the matter;
- e) Put in place measures to ensure that employees are made aware of the legislation and related policies, procedures and controls;
- f) Ensure that relevant employees are appropriately trained on a regular basis in the recognition and handling of suspicious transactions;
- g) Provide for compliance management arrangements; and
- h) Ensure independent and regular auditing of the internal policies, procedures and controls established and carried out.

Accountants and auditors are required to establish written internal reporting procedures, which will enable employees, directors or partners to know to whom they will report any knowledge or suspicion of ML/TF/PF activities. This means they have first to appoint MLRO to whom the report shall be made. The MLRO shall be a senior officer to be able to liaise with the management and other employees on matters related to ML/TF and shall have reasonable access to any other information which is readily available and that may be of assistance to him.

The MLRO appointed among other things is required to monitor transactions and ensuring compliance with the AML/CFT legislations. The role of the MLRO carries significant responsibility in AML/CFT regime and should be undertaken by an appropriately experienced individual with sufficient authority to enable decisions to be taken independently. In addition, MLRO is required to:

- a) Consider internal reports of money laundering and terrorist financing
- b) Act as the liaison point with FIU

⁸ Without delay as per regulation 3 of POTA Regulation means within a matter of hours after designation or within such a time to prevent flight or dissipation of funds or other assets of the designated party or within such time before the designated party or any other relevant or concerned person becomes aware of the designation or within such time to allow concerted action to swiftly interdict and disrupt their flow.

⁹ As per section 41A of POTA, CAP 19

¹⁰ Tipping off is an offence under section 20 of AMLA, CAP 423

- c) Advice on how to proceed with work once an internal report has been issued to guard against risks of tipping off or prejudicing an investigation;
- d) Design and implementation of internal reporting procedures.
- e) Maintain AML policy
- f) Putting in place necessary controls for detection of suspicious transactions.
- g) Receiving disclosures related to suspicious transactions from the staff or otherwise.
- h) Prepare training program on AML/CFT and ensure all relevant staff are equipped with necessary knowledge to assist establishing factors for the detection of suspicious transactions.
- i) Coordinate Preparation of CDD requirement checklists for all type of clients
- j) Coordinate ML/TF risk assessment for clients.

The MLRO can appoint an alternate to assist him/her in fulfilling his/her obligations, although this does not relieve that MLRO of his responsibility. It is for accounting and auditing firms to determine the format of their internal reports but reports to FIU must be made in pursuance to section 17 of the Act and Regulation 22.

10. TERRORIST FINANCING SANCTIONS

10.1 Protection from Liability

The AML/CFT provisions discussed in section 8.2 to 8.4 of these guidelines regarding the reporting of suspicious transaction, cash transaction, terrorist property and the disclosure part provided in section 3.0 of these guidelines involving the affairs of clients override the fundamental principle as provided in Section 140 of the IFAC code of ethics for Professional Accountants to the effect that accountants and auditors should not disclose to third parties, information acquired as a result of professional or business relationship without the client's consent.

On the other hand, the new standard in regard to Non-Compliance with Laws and Regulations (NOCLAR) sets out a first-of-its-kind framework to guide accountants and auditors in what actions to take in the public interest when they become aware of a potentially illegal act, such as involvement in bribery and tax evasion or to breaches of laws and regulations, committed by a client or employer.

It is obvious that disclosure of client's information if not made in good faith may result into breach of trusts and confidentiality principle. **Accountants and auditors must understand and observe that any reporting or disclosure in compliance with any provision in AML/CFT requirements will not be counted as breach of any restriction on the disclosure of information (emphasis added).** A report or disclosure made in relation to the following will be considered as "protected disclosure";

- a) Suspicions on transaction or proposed transaction related to tainted property or predicate offence,
- b) Information that assists for arrest or prosecution of persons accused for terrorist and terrorist financing,

- c) Information that may be of an assistance in preventing the commission of an offence, and
- d) Information that discloses existence of the tainted property.

Accountants and auditors should note that any reporting obligation in relation to ML/TF must be in circumstances where the information has been accessed in the course of business. On the other hand, disclosure of information in relation to terrorist or terrorist financing do not require accessing information in the course of business, whereas, the requirement is to be acquainted with the information and forthwith disclose to Police officer or FIU.

The AML/CFT regime provisions that protect *Bonafede* disclosure are provided hereunder;

Section 22 of AMLA

- (1) *Notwithstanding any other written law, no action, suit or of other proceeding shall lie against any reporting person or any director, officer, employee or representative of the reporting person on grounds of breach of banking or professional secrecy or by reason of any loss resulting from an investigation, prosecution or other legal action taken against any person, following a report or information transmitted in good faith under this Part whether or not the suspicion proves to be well founded.*
- (2) *In any criminal proceedings brought under this Act, the court may, upon an application by the Director of Public Prosecutions, order:*
 - a) *Witness testimony to be given through the use of communication technology such as video conferencing;*
 - b) *Non-disclosure or limitations as to the identity and whereabouts of a witness taking into account the security of the informer or witness; or*
 - c) *Any other protection as the court may upon application by the Director of Public Prosecutions, order.*

Section 40(3) of POTA

No civil or criminal proceedings shall lie against any person for disclosing any information, in good faith, as required under sub section 1.

Section 41(4) of POTA

No civil or criminal proceedings shall lie against any person for disclosing or reporting any information, in good faith, as required under sub section 1 or 2 or 3.

Section 41A (4) of POTA

No civil, administrative or criminal proceedings shall be instituted against a reporting person for making disclosure or report, in good faith, or as required under section 41 and this section.

11.0 STAFF TRAINING AND TRAINING PROGRAMMES

All employees of the accounting and auditing firms must be trained about the policies and procedures relating to prevention of money laundering, provisions of the AML/CFT legislations and the need to monitor all transactions to ensure that no suspicious transaction is being undertaken under the guise of money laundering. Accounting and auditing firms should have an ongoing training program for consistent implementation of the AML/CFT measures and steps to be taken to guide an accountant or auditor when comes across with any suspicious transaction(s) while performing his professional duties.

Section 19 of the AMLA, Cap 423 provide that all relevant employees are required to be made aware of law relating to money laundering and terrorist financing, and regularly given training in how to recognize and deal with transactions which may be related to money laundering or terrorist financing. In considering, a training program need to keep in mind the objectives they are trying to achieve, which is to create an environment effective in preventing money laundering and terrorist financing and which thereby help protect individuals and the firm. In particular, MLRO and members of senior management may require supplementary training in a customized approach.

In general, employees at a minimum must be aware of the following:

- a. The company's anti-money laundering policy.
- b. A description of the nature and processes of money laundering.
- c. An explanation of the underlying legal obligations of both the employee and employer under the anti-money laundering law, regulations and guidelines;
- d. An explanation of the existing system to prevent and detect money laundering and terrorist financing with particular emphasis on the recognition of suspicious transactions and the submission of suspicious transaction reports to the MLRO in a timely manner.

Case study 1

Money Laundering

Facts of the Case

Mr. Andreou is an accountant and an administration service provider regulated by ICPAC, working in Cyprus. Mr. Andreou had employed one Compliance Officer (CO) who is a recently qualified accountant with no AML experience and limited work experience. Mr. Smith from the UK, who owns a used car dealership in the UK, approached Mr. Andreou and requested for bank administration and accounting services. Mr. Andreou sets up a company with the assistance of a registered licensed lawyer that purchased used cars from Mr. Smith's UK Company and resold them in the local market. Mr. Andreou approved and processed the payments of the purchases and members of his staff issued the sales invoices and deposited the receipts from the sale of the new cars and maintained proper accounting records. The business was very profitable and cash rich, as the used cars were bought at a very low price and resold at a significantly higher price in cash.

One employee of Mr. Andreou expressed her concerns to the CO as she was worried that the majority of sales were made in cash (below the €10,000 threshold¹) and, in addition to this, in many instances the cars were registered to a different customer than the one paying for the sale. The CO dismissed her worries and explained that this is how business is done in Cyprus, and that many people still have cash at home after the deposit haircut in 2013.

Not long after, Mr. Smith was convicted and imprisoned, since it emerged that he is a drug dealer who has set up used car sale businesses in a number of countries to launder the proceeds from drug sales. As a result, all used cars and cash were viewed by the Republic of Cyprus as criminal proceeds and were now the subject of confiscation proceedings.

Mr. Andreou was arrested and put on trial alongside the Compliance Officer. According to the prosecution, the set up and management of the company was intended to eliminate the trail that led back to Mr. Smith and his illegitimate funds and they should have been suspicious of the transactions as the cars sold were almost obsolete but generated high income in cash. The CO and Mr. Andreou claimed they had no knowledge that the cars were in such a poor state and did not have grounds to suspect Cypriot buyers using cash to settle their purchases.

The CO was convicted of failure to report, contrary to Article 27 of the Prevention and Suppression of Money Laundering and Terrorist Financial (Amending) Law of 2018 (the "Law") and sentenced to 12 months' imprisonment.

1. Where are the red flags?

- The sale of the used cars at a premium price
- The volume of cash receipts
- The registration of the car under a different name from the buyer's name

2. What actions should have been taken?

- Before accepting the client, proper KYC should have been performed followed by the risk assessment that would have enabled the CO to ascertain what sources and quality of evidence is required during the due diligence.
- If proper source of fund/wealth was established and the economic profile of the client had been properly constructed prior to the execution of the transaction, the origin of the funds might have been exposed as resulting from illegitimate activity.
- It would also have been expected that if an appropriate senior executive with skills, knowledge and experience was appointed as the CO of the company (as required by the AML Law, article 69(1)), he would have become suspicious when the accountant had alerted him of such transactions and been able to question the rationale of the transactions and picked up the red flag.
- The firm should also have had policies in place to guide the staff on how to report suspicion internally to the CO and any considerations/explanations should have been documented.
- Finally, the CO should have filed a Suspicious Activity Report (SAR) with MOKAS.

Case study 2

Insufficient and unsatisfactory KYC documents

Facts of the Case

Maria is the Compliance Officer of the Best Audit Firm Ltd. She is in charge of meeting with all new prospective clients and obtaining all necessary information before the commencement of the business relationship.

A new client, Mr. Shamir, introduced by a long-standing existing client, has come in the office for a meeting. Mr. Shamir is an Israeli resident, a Cyprus home owner with a company that trades in furniture. Maria went through all the KYC documents required for the onboarding, explained the company's policies and procedures to be followed and left the meeting with a promise that the prospective client will provide all documents within the end of the week, so the firm can proceed with its acceptance procedures

Mr. Shamir, as promised, dropped off at the reception an envelope with some documents, but upon review, Maria realized that he had only provided a few documents. She emailed him a list of missing documents and a new deadline to provide her with everything. Mr. Shamir responded that he was in a hurry to obtain a Tax Identification Number and requested the firm to proceed with the application to the Inland Revenue until he comes back next week with the necessary documents.

The firm prepared the forms to be submitted to the Inland Revenue and asked him to come in the office and sign the forms and bring the remaining documents. Mr. Shamir signs the documents and leaves a substantial cash amount to the firm for future services but omits to bring in the pending documents required to complete the KYC and Due Diligence procedures. He explained that the documents are held by his lawyer and he has not passed by his office to collect them.

Maria contacts the client who referred Mr. Shamir to the firm and finds out that he does not know him that well and that he arrived from the illegitimate airport of the occupied area of Cyprus. Maria contacts Mr. Shamir immediately and asks him for a meeting. Mr. Shamir fails again to provide the firm with the missing documents, he explained that he does not have a utility bill for his Cyprus residence which had been marked as his main residence and that his yellow slip (residence permit issued from the immigration office) is held by the lawyer. As a result, Maria informed him that Best Audit Firm Ltd cannot provide any services to him and returned the cash to him. No further services were provided to Mr. Shamir.

1. What are the red flags, which might indicate money laundering activity and/or terrorist financing in this case?

- Mr. Shamir would not provide the documents requested by the compliance officer
- The urgency of Mr. Shamir to proceed with the registration to the Inland Revenue
- The substantial cash paid to the firm for future work
- The entrance into the country through the occupied area of Cyprus.

2. What are the risks and potential threats that the accounting firm may be faced with in this situation?

- The firm could have unknowingly been assisting in a money laundering/terrorist financing scheme through the inability to verify the client
- Reputational risk
- Administrative fines for not performing adequate due diligence

3. What actions should the Compliance Officer have taken?

- The Compliance Officer should have assessed whether the prospective client's unwillingness to provide the necessary documents was suspicious and report the case to MOKAS
- The firm should not have proceeded in offering any services to, or accepting any cash payment from the prospective client before the completion of the Due Diligence ("DD") / Know Your Customer ("KYC") process.

Case study 3

Investment fraud

Facts of the Case

An investment company is offering brokerage service to clients. It collects clients' funds and places them into the bank account denominated as "Clients Bank Account" with ABC Bank plc, for further clearing and settlement transactions for clients' orders, which require 2 signatures of both executive directors.

Clients' agreement indicates that the Company does not use clients' funds for own purposes, separates and segregates clients' funds in an EU bank.

The Company has a process to daily reconcile the records of accounting, back office and bank, to ensure that the Clients' Funds are kept in the separate accounts with the licensed bank and not used for 'own' Company needs at any circumstances.

Due to shortage of staff, the in-house accountant is responsible to prepare accounting records, which include obligations to clients, and to reconcile these records to third party records and to back-office records.

Due to non-compliance with the risk management policies, and resulting liquidity and capital shortage, executive directors decide to use clients' funds to hedge own trading positions.

Trading, unfortunately, is not profitable and the clients' funds are paid to the counterparties to settle own loss-making trading deals.

The in-house accountant, due to heavy workload, prepares the accounting records based on the accounting statements, however, does not perform regular reconciliations with the back-office records, to ensure that the Clients' funds held with the ABC Bank and reflected in the accounting records, correspond to the amounts reflected on clients' statements (i.e. what Company shows in external reports to clients as due to clients).

At some point, the clients start to experience difficulties in withdrawing the funds and complain to the Competent Authority.

The Competent Authority during its investigation revealed that the company:

- Committed a theft of clients' funds and used them for own purposes,
- Operates a scheme where the clients' withdrawals were paid from other's clients funds generated by aggressive marketing techniques,

- Did not employ the procedures to safeguard clients' funds,
- Internal 2nd and 3rd line of controls failed to report this to the Board and to the Competent Authority.

As a result, the Company's license is withdrawn due to non-compliance with Article 28(1) of the Law, in relation to the authorization and operating conditions laid down in Article 18(2)(j) of the Law, was due to their fault, willful omission and negligence.

1. Economic crimes committed

- Theft (of clients' money)
- Fraud (pyramid-style payments)
- Conspiracy to commit fraud (executive directors acted in concert for bank signature purposes)
- Furnishing false information to clients
- Money laundering

2. Actions made by the professionals to enable these crimes?

- The executive directors forced the Company to commit theft by transferring clients' funds to own accounts and giving instructions to settle own obligations with clients' funds.
- The in-house accountant assisted in fraud and theft, by being negligent for nonperforming the required tasks.
- Internal Audit, AML and Compliance functions failed to recognize, and report risks due to negligence.

3. What actions might the in-house accountant have taken?

Firstly, the accountant should ensure adherence to the procedures set and should perform regular reconciliations in the prescribed format.

Secondly, if the task could not have been performed due to the workload, this should have been escalated to management and control functions. By elevating the issue to senior management, further resources would possibly have been devoted to the accounting function. In case, management was reluctant to do so then the accountant:

- Should resign due to inadequate resources to properly performance his duties (per section 330.2 of IFAC Code of Ethics for Professional Accountants).
- Based on his judgement and professional skepticism, he should seriously consider reporting the suspicion by submitting a Suspicious Transaction Report to the Anti- Money

Laundering Officer appointed in accordance with the Regulators Directives for the prevention of money laundering, as per the firm's standard AML procedure.

Thirdly, by performing proper and accurate reconciliations on a regular basis, the accountant could have realized that the Company's management uses clients' funds for own purposes and that Clients' funds are stolen.

In this case, if the accountant believed that others are behaving or acting unethically, he should first consider raising the matter internally, through the organization's own whistle-blowing procedure, by submitting the Suspicious Transaction Report to the Anti-Money Laundering Officer appointed in accordance with the AML Law.

Alternatively, he may wish to seek the advice of his professional body and/or a lawyer or the regulator.

If all the available options for reporting and escalation have been exhausted, the in-house accountant might finally conclude that it is appropriate to resign.

4. Role of Professional accountants in such cases.

The professional accountants can help prevent fraud and theft using their expertise, professional skepticism and their professionalism to act with integrity and by refusing to become associated with practices they know to be unethical or contrary to the law and regulations.

Their role goes beyond this as they are expected to educate staff, peers and management within the organization for the proper adherence of firm's policies and procedures in respect of the accounting function and of any exceptions they may identify during the conduct of their work (reconciliations of clients' accounts, recording and reviewing of transactions and balances). Accountants have the necessary skills and position to explain the risks and potential consequences of unauthorized use of clients' assets.

Established compliance processes should, in all likelihood, be in place and work as prescribed.

Case study 4

Money Laundering

Facts of the Case

Yiannis is an in-house accountant of a Cyprus incorporated company (“the Company”) which is a subsidiary of a large group of companies incorporated in Russia. He is a professional accountant and an expert in financial instruments. Further to the company working hours, Yiannis is working until late regularly during which time he processes the major part of the company’s transactions.

More specifically, he is using a few bank accounts, which were opened in the name of the Company, to carry out transfers in foreign currencies. In most of the cases these activities are not linked to the business activities of the Company. In addition, the balance of the accounts is usually nearly zero; however, the total amount of the transfers and volume of transactions is often considerable.

The transactions posted in the general ledger are split in small amounts and in addition, many of the transactions are rounded amounts and less than €1.000. The internal policy of the company is to supervise transactions which are above €1.000. The proceeds from the transactions are deposited at different branches of the same bank.

Also, he makes short-term investments, mainly using electronic means to transfer, in marketable securities and derivatives, which are quickly liquidated so that the proceeds can be reinvested. The investments are spread in Bermuda, Seychelles and Mauritius and other locations around the world.

Yiannis behavior has been identified by some other employees of the Company, but without taking any further steps or informing any person of the Company high on the hierarchy. The company recently hired a new accountant supervisor to assist the financial controller of the Company and he suspects that Yianni’s transactions are outside the corporate goals of the Company and its activities and seems not to be legitimate transactions.

1. What red flags can we observe in the above scenario?

There are numerous red flags in the scenario but the obvious one that is often over looked is the employee working until late regularly and possibly does not take vacation. Yiannis is working until late regularly, where a large volume of transactions is being processed. The absence of any obvious explanation for the late working hours environment could be a sign that they are being deliberately set up to confuse and obscure. The use of several bank accounts for transfers which in most cases are not linked to the main activities of the Company maybe another indication of money laundering.

Additionally, the bank accounts closing balance on each day is close to zero even though the total amount and volume of transactions is considerable. Moreover, the posted transactions are below the threshold of €1.000 which is the Company’s threshold for requiring supervision on transactions executed and entered into the system.

Finally, complex financial instruments, derivatives in this case, being used by a business with no obvious business rationale is a sign of the layering and integration stages of money laundering.

2. What can professionals do to combat criminals and fraudulent activity? What tools do they have at their disposal?

Professional accountants are usually in a position to assist the financial intelligence units and the economic crime department of the police to identify and eliminate criminals and fraudulent activity. Very often, processing any single or number of transactions requires the involvement of several advisors. These could include but are not limited to corporate service providers, brokers, forensic accountants and fraud auditors;

Professional accountants have a duty under the AML legislation to file a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) to The Unit for Combating Money Laundering (“MOKAS”), whenever they suspect a crime under the AML Law. SARs and STRs include details of all parties, the suspicious transactions, the history and the trail.

MOKAS has implemented the go AML software for easier and more efficient reporting. The Institute of Certified Public Accountants (“ICPAC”) Prevention and Suppression of Money Laundering Activities Directive (the “Directive”) Par. 2.09 requires their members to report to MOKAS acquired knowledge or reasonable suspicion that another person is engaged in money laundering or terrorist financing. No offence of tipping-off is committed when the disclosure is made in this way to MOKAS or to competent Supervisory Authorities under Article 69 of The Prevention and Suppression of Money Laundering Activities (Amending) Law of 2018 and Par. 2.10 of the Directive.

3. What are the obligations of an ‘in-house accountant’?

Any direct involvement of the accountants in the money laundering process means that they are themselves breaking the Law.

Additionally, any person, including an auditor, external accountant, tax advisor or trust and company service provider, in practice or elsewhere, who, in the course of his trade, profession, business or employment, acquires knowledge or reasonable suspicion that another person is engaged in money laundering or terrorist financing, commits an offence if he/she does not report his/her knowledge or suspicion to MOKAS, as soon as it is reasonably practical after the information came to his/her attention. This duty to report arises under Article 27 of the Law and Par. 2.09 of the Directive.

Adherence to the Code of Ethics for Professional Accountants is fundamental in the obligations of and in-house accountant. This promotes professional integrity, which provides the means to protect against complicity in economic crime and acts as a barrier against (un) professional enablers and even protects against unintentional participation in an economic crime.

In this case, the accountant is in clear breach of the Law as well as the Directive and the Code of Ethics for Professional Accountants. He did not demonstrate any professional skepticism and integrity and disrespected the company policies and the principles of the law and the Code.

Case study 5

Complex structures

Facts of the Case

An accounting firm is offering administration, bookkeeping and corporate services to a large Group with a corporate structure consisting of a number of companies whose main activities are the holding of investments in various industries and the provision of consulting and management services.

The fees generated by the accounting firm from this Group amount to 5% of the firm's annual turnover.

The companies belong to a large Group consisting of companies registered in various low tax jurisdictions. Although different shareholding percentages apply to the various layers of the structure, the Group seems to belong to a number of trusts which are set up, again, in various jurisdictions.

The accounting firm suspects that there may be other companies belonging to the same Group which may be administered by other service providers in Cyprus, but this information could not be verified with certainty.

Overall, there seems to be a tendency for secrecy when the employees of the accounting firm seek to obtain information and documentation from the people acting as the representatives of the Group. Furthermore, information on the beneficial ownership and control of the structure is somewhat obscured, although, the accounting firm suspects that the whole structure belongs to a Ukrainian multimillionaire and his family who has interests in a number of different industries and holds key positions in the Board of Directors of major Ukrainian companies and is also known to have close links with the government.

The accounting firm, despite numerous efforts, only now managed to receive the necessary documentation in order to carry out the bookkeeping of these companies for the last three consecutive years and this documentation revealed the following:

The investments in various companies, especially start-ups, are acquired and are disposed of within a short period of time always at a profit.

- The companies of the Group have numerous bank accounts both in Cyprus and abroad and funds are being transferred between these bank accounts immediately upon deposit.
- The invoices for consulting and management services are predominantly issued to Ukrainian companies. The accounting firm accidentally found out that the Ukrainian multimillionaire is a member of their Board of Directors.

1. What are the red flags which might indicate money laundering activity and/or terrorist financing in this case?

- Rapid disposal of investments.
Swift transfers of funds between bank accounts of the various companies and other entities of the Group.

- Complex structure! Why? What is the purpose?
- The fact that the ownership structure is not clear should raise concerns. Does the accounting firm have access to all records of all entities in the structure especially the documents relating to the trusts? And more specifically who is the settlor (his Source of Wealth and Source of Funds) and the beneficiaries?
- The fact that the companies administered by the accounting firm in Cyprus receive consultancy fees from Ukrainian companies, for which the purported UBO acts as a Board Member, should raise concerns as to whether the transactions are done at arm's length, or whether there are suspicions for tax evasion, bribes or any other type of money laundering.

2. What are the risks and the potential threats that the accounting firm may be faced with in this situation?

- Significant fees earned from this structure. Therefore, fee dependency which could lead to discounts in various compliance processes.
- The Group invests in various industries. The accounting firm may not have the necessary expertise and knowledge to be able to better understand and handle these activities.
- The wide dispersion of the Group in various low tax jurisdictions. The accounting firms may be unaware of the reasons for such dispersion and hence the hidden reasons as to the complexity of the structure.
- The fact that the accounting firm suspects that another part of the same Group is being serviced by another firm in Cyprus. Why would this be necessary or undisclosed?
- The tendency for secrecy by the client's representatives. Are there issues which are not disclosed to the accounting firm and hence pose a threat?
- The risk of not properly establishing who the real UBO is and his/her source of funds.
- The unverified information that the Group may be owned by a Ukrainian multimillionaire having links with the Ukrainian government. If the real owner is indeed to Ukrainian multimillionaire with ties to the government, the Group should be treated as PEP related, due diligence should be performed as to the reason of setting up the complex structure and the economic reason of the transactions performed.
- Delay in receiving the necessary information to prepare the financial statements despite numerous follow-ups. There is a possibility that the documents are manipulated.
- The accounting firm may find itself unwittingly being assisting in a money laundering/terrorist financing scheme. Indicators:
- Investments are being made in various companies and being disposed within a short period of time.
- Many investments are being made in start-ups, whose value cannot be easily measured.
- Money is transferred in numerous accounts in Cyprus and abroad, immediately after deposit.
- May be exposed to investigation as a result of possible wrong doing by its client.
- May be subject to disciplinary action by the regulator and the court.

3. What KYC/Due Diligence work should the accounting firm have carried out and when?

- Clear establishment of the actual UBO. In this respect the Group structure should be obtained and relevant corporate documents reviewed (including trust agreements).
- Once the UBO is identified the firm should perform full KYC/DD on the individual UBO (i.e. identification, utility bill). Searches should also be carried out on the Group and the UBO against sanctions / PEPs lists, and in various internet sites to establish the background, Source of Funds and Source of Wealth of the UBO and the Group. References should also be obtained from independent reliable sources.
- Establish whether there is a valid economic purpose for setting up such a complicated structure.
- Establish the expertise possessed by the UBO and/or directors of the Group to be able to operate in the industry within which the company is operating.
- Obtain detailed information as required by the Law and the Directive on any of the Trusts that appear in the Group structure.

4. What steps could the accounting firm undertake to mediate its risks and possible exposure?

- Immediately re-perform KYC/DD on the Group, establish who the UBO is and perform KYC/DD on the UBO.
- Immediately perform KYC/DD on the company's counterparties especially in relation to the loans granted and the services provided.
- Carry out detailed search in relation to the company's investments.
- Scrutinize all agreements entered into by the Group.
- Address these queries to the representatives of the Group, in order to obtain the necessary answers.
- Consider filing a report to MOKAS, if suspicions for ML/TF arise.

XX