ICPAK
Credibility. Professionalism. Accountability

Anti-Money Laundering Guide for Accountants in Kenya

Supported and funded by

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

September 2020

Contents

Interpretation

For the purposes of this Guide, the following abbreviations will mean:

ACR	–	Annual Compliance Report
Act	–	Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009
AQR	–	Audit Quality Review
Branch Office	–	An office location in Kenya, other than the main office, where business is conducted
CDD	–	Customer Due Diligence
Center	–	The Financial Reporting Center established under section 21 of Proceeds of Crime and Anti-Money Laundering Act, 2009
Confidentiality	–	has the same meaning as defined in the International Code of Ethics for Accountants issued by the International Ethics Standards Board
EDD	–	Enhanced Due Diligence
DNFBPs	–	Designated Non-Financial Businesses or Professions
ESAAMLG	–	Eastern and Southern Africa Anti Money Laundering Group
FATF	–	The Financial Action Task Force
FIU	–	Financial Intelligence Unit
FRC	–	The Financial Reporting Center
FSRBs	–	Financial Action Task Force-Style Regional Bodies (FSRBs)
ICPAK	–	The Institute of Certified Public Accountants of Kenya
ML	–	Money Laundering
MLRO	–	Money Laundering Reporting Officer
MLTF	–	Money Laundering and Terrorism Financing
Numbered Account	–	Accounts where the identity of the holder is replaced with a multi-digit number known to the client and private bankers only
OFAC	–	The Office of Foreign Assets Control
PEP	–	Politically Exposed Person
PIP	–	Prominent Influential Person
RBA	–	Risk Based Approach
Regulations	–	Proceeds of Crime and Anti-Money Laundering Regulations, 2013
SAR	–	Suspicious Activity Report
Search warrant	–	A formal permission granted to law enforcement agencies by a court of law to search designated premises and or seize certain documents
STR	–	Suspicious Transaction Report
TF	–	Terrorism Financing

Forward

The money laundering landscape continues to evolve, often posing a threat to national security from large criminal funds being laundered. While bankers have traditionally been the focus of Anti-Money Laundering (AML) legislation, the role of other professionals, including accountants, is becoming increasingly critical. Accountants in Kenya are at risk of penalties (both monetary and criminal) for non-compliance with local and international Anti-Money Laundering (AML) Legislation.

An effective AML compliance program is key to mitigating this risk. Thus, pursuant to Sec 8(f) of the Accountants Act, as read together with Sec 24A (3) of the Proceeds of Crime and Money Laundering Act, the Institute of Certified Public Accountants of Kenya (ICPAK) has commissioned this Guidance document to help accountants in Kenya deal with recent changes in AML regulatory requirements as well as emerging Money Laundering and Terrorism Financing (MLTF) risks. Section 24 A (3) of POCAMLA grants the Financial Reporting Centre authority to delegate powers to a supervisory body to issue instructions, directions, guidelines or rules regarding the application of the Act to reporting institutions regulated or supervised by the supervisory body.

The guideline therefore is designed to reduce the possibility of the accountancy profession being knowingly or unknowingly used for purposes connected with an offence involving proceeds of crime, fraud, theft or money laundering as defined under POCAMLA. These Guidelines are hereby issued with the approval of the FRC.

This publication aids Accountants together with their practices or employing organizations to addressing comprehensive topics including: Key definitions and applicable regulations, Money laundering risk assessments and the risk based approach, Obligations of Accountants in practice and those in business, Customer due diligence, Suspicious activity / transaction reports, Record keeping, Training, and Regulatory Examination.

The Guide has references to the Financial Reporting Centre, which provides checklists, forms and offers practical guidance on how to complete such forms. Consequently, the Guide may be amended periodically as and when necessary.

On behalf of ICPAK Council and on my own behalf, I wish to sincerely commend the Chief Executive Officer and Public Policy and Research Division for their commitment in conceptualizing and actualizing the development of this Guide. I also wish to express our gratitude to the Financial Reporting Centre, Flywheel Advisory Africa and all the stakeholders who participated in any stage of the development of this Guide for their invaluable input and comments. Lastly, I wish to take this opportunity to more sincerely thank GIZ for their partnership and continued financial support to this project.

FCPA Rose Mwaura, MBS

Chairman,

Institute of Certified Public Accountants of Kenya

Acknowledgement

The Institute takes this opportunity to recognize and acknowledge the significant contributions by Gilbert Ouko and Grace Mburu of Flywheel Advisory Africa in the development of this guide. The Institute further acknowledges the expert input and guidance of various Committees and subcommittees in ensuring this guide addresses the fundamental issues of applicable regulations, risk assessments, obligations and Regulatory Examination. To this regard, we sincerely appreciate the Public Policy and Governance Committee and Legislative Affairs Committee Workstream for their contribution and validation during the development of this guide.

We also express sincere gratitude to the Secretariat under the able leadership of Hillary Onami, Elias Wakhisi, Evance Juma, Nancy Moraa and Everlyne Maingi for their input and delivery of this guide. The Institute further appreciates the input and support of the Financial Reporting Centre led by Mr. Saitoti Maika the Executive Director and Mr James Manyonge, the head of legal services.

We express our sincere appreciation to everyone who in one way or the other participated in the development of this guide. Special tributes to CPA Nixon Omindi and CPA Samuel Kiragu for their invaluable input. Lastly but not least, we forever remain indebted to the funding and support of GIZ.

CPA Edwin Makori

Chief Executive Officer

Institute of Certified Public Accountants of Kenya

1 About this Guide

- Introduction
- What is the objective of this Guideline?
- Triggering activities - To whom is this guide applicable?

1.1. Introduction

1.1.1 The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009 and its regulation (the proceeds of crime and anti-money laundering Regulations, 2013) makes it mandatory for reporting institutions to report any transaction related to money laundering to the Financial Reporting Centre. The mandatory reporting prescribed in POCAMLA is designed to assist in the detection and prevention of money laundering activities, as well as to facilitate the investigation and prosecution of money laundering offences.

1.1.2 The Institute of Certified Public Accountants of Kenya (ICPAK), being a supervisory body under the Act, has prepared this document to provide guidance to Accountants engaged in triggering activities as defined under POCAMLA (Section 48) when performing their duties.

1.1.3 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 Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009.

1.1.4 In performing their obligations, individual Accountants and/or their practices are advised to read local and international Acts and Regulations from various bodies influencing the MLTF requirements. These include but not limited to:

- The Proceeds of Crime and Anti Money Laundering Act, 2009 (POCAMLA);
- The Prevention of Terrorism Act, 2012 (POTA);
- The Institute of Certified Public Accountants of Kenya (ICPAK) Code of Ethics for Accountants;
- Financial Action Task Force (FATF) 40 Recommendations;
- FATF-style regional bodies (FSRBs) such as Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) guidelines and topology reports;
- The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury actions; and
- Egmont Group of Financial Intelligence Units (FIUs) guidelines and topology reports.

1.2. What are the objectives of this Guideline?

1.2.1 Section 24 A (3) of POCAMLA grants the FRC authority to delegate powers to a supervisory body to issue instructions, directions, guidelines or rules regarding the application of the Act to reporting institutions regulated or supervised by the supervisory body.

1.2.2 The Institute as supervisory body in collaboration with the Financial Reporting Centre has prepared this guideline on Anti-Money Laundering for accountants to enlighten its members on their obligations under the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009.

1.2.3 The guideline is designed to reduce the possibility of the accountancy profession being knowingly or unknowingly used for purposes connected with an offence involving proceeds of crime, fraud, theft or money laundering as defined under POCAMLA.

1.3. Triggering activities - To whom is this guide applicable?

1.3.1 This Guideline is intended for use by any persons registered as an accountant in Kenya, whether in public practice or in business, together with their practices or employing organizations when preparing or carrying out transactions for their clients in the following situations:

- Buying and selling of real estate;
- Managing of client money, securities or other assets;
- Management of bank, savings or securities accounts;
- Organization of contributions for the creation, operation or management of companies; or
- Creation, operation or management of buying and selling of business entities.

1.3.2 Local and foreign branches of institutions (where applicable), are considered not to be legally distinct from their head office and are therefore subject to POCAMLA. Failure by a branch to comply with POCAMLA and its regulations will be considered as a failure to manage group risks, which may result in action being taken by the Financial Reporting Centre and the professional regulatory body - ICPAK (See 3.7) either severally or jointly. See Regulation 23 of the POCAMLA Regulations.

1.3.3 This Guidance is not intended to be exhaustive. It should be read together with The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009 and its regulation (the Proceeds of Crime and Anti-Money Laundering Regulations, 2013), the Accountants Act, as well as the ICPAK Code of Ethics for Accountants.

2 Definitions

- Who is an Accountant?
- What is Accountancy?
- What is Money Laundering?
- What is
- POCAMLA
- POTA
- Risk Based Approach (RBA)

2.1. Who is an Accountant?

2.1.1 An "accountant" is a person registered as an accountant under Section 24 of the Accountants Act and is a member as defined in section 4 (2) (a) and (b) with expertise achieved through formal education and practical experience, and shall be held to a high professional standard in respect to —

- demonstrating and maintaining competence in accountancy in line with International Accounting standards;
- compliance with the Institute's code of ethics;
- maintaining good standing status; and
- subject to enforcement of the rules and regulations of the Institute;

2.2. What is Accountancy?

2.2.1 The Accountants Act 2008 defines "accountancy" means practice in accounting, financial reporting, control systems, systems auditing, auditing, assurance, forensic accounting and auditing, finance, financial management, public finance management, taxation, financial risk management, management accounting and advisory services related thereto

2.3. What is Money Laundering (ML)?

2.3.1 The POCAMLA defines "Money Laundering" as an offense under sections 3, 4 and 7 of the Act. These are:

- Entering an agreement, engagement or transaction in connection to a property that is or forms part of the proceeds of crime (POCAMLA Section 3);
- Acquisition, possession or use of proceeds of crime (POCAMLA Section 4); and
- Any financial promotion of an offence such as transporting, transmitting, transferring or receiving

a monetary instrument or anything of value with intent to commit an offence as defined in the Act (POCAMLA Section 7).

- Please see the Act for detailed definition. The meaning given in this Guide is a simplified version of the definition given by the Act.

2.3.2 Money Laundering takes place in 3 stages:

- ***Placement*** - The introduction of cash or other assets illegally obtained into a financial institution. It may take the form of repayment of legitimate loans with laundered cash, blending of clean and dirty money in cash intensive business as supermarkets and restaurants and depositing small amounts of the laundered cash into a bank just below the reporting threshold.
- Layering - Creating complex layers in movement of cash to disguise its source and audit trail. This may involve converting cash into monetary instruments, purchasing bonds and stocks, electronic movement of funds into other countries as well as investing in real estate. Layering may also occur in scenarios where, after funds are deposited into the account, internal transfers are initiated, or money loaded to prepaid cards.
- Integration - Re-entry of criminal funds into the economy in what appears to be proceeds from legitimate sources. It may involve the purchase of luxury property, jewelry and automobiles.

2.3.3 It is during the layering and integration stages where Accountants are highly at risk of being knowingly or unknowingly used as accomplices of money laundering acts. It is also important to note that money laundering does not necessarily follow the three stages in any specific order.

2.3.4 POCAMLA has created other offences related to money laundering including:

- Willful failure to report a suspicious transaction by obligated persons (Section 5);
- Financial promotion of ML (Section 7);
- Tipping off (Section 8);
- Misrepresentations to a reporting institution, supervisory body or the FRC (Section 9); and

- Making malicious reports (Sections 10).
- See 2.7.9, 2.7.10 and 9.1 for guidance on implementing a Risk Based Approach and red flags for potential MLTF cases.

2.4. What is Terrorist Financing (TF)?

2.4.1 Recommendation 5, of the Financial Action Task Force (FATF) defines terrorism financing as the provision of funds, whether legal or illegal to aid a terrorist activity, funding the lifestyles of the terrorists, aiding movements of arms from one jurisdiction to another, proliferation of arms and their storage.

Kenya's Prevention of Terrorism Act (POTA) 2012 Section 5 defined Terrorist Financing as the collection (or attempting to collect), provision (or attempting to provide) or inviting a person to provide or make available property, funds or services intending, knowing or having reasonable grounds to believe that such property, funds or services shall be used for the commission of a terrorist act or to benefit a person involved in a terrorist act. See POTA Part 3 for further definition and offenses under POTA.

2.4.2 The difference between Money Laundering (ML) and Terrorist Financing (TF) is that funds in money laundering are always proceeds of a criminal activity whereas in the latter, funds can be from legitimate or illegitimate sources but their purpose is illegal. Kidnapping for ransom, drug trafficking, extortion, human trafficking, sex trafficking, modern slavery and even fraud are ways in which terrorists raise funds to carry out their activities illegally. On the other hand, legitimate sources as charitable contributions to Non-Government Organizations, membership dues and sale of publications may be misused as a disguise to fund terrorist activities.

2.4.3 It is important to note that terrorist financing transactions may not be easily detected as they are often in small amounts, hence fail to trigger any reporting action.

See 2.7.9, 2.7.10 and 9.1 for guidance on implementing a Risk Based Approach and red flags for potential MLTF cases.

2.5. What are the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA)?

2.5.1 The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) is the Kenyan comprehensive AMLTF Act. The Act was developed in 2009 to guide how anti-money laundering cases are to be identified and reported, as well as associated offences and penalties.

2.5.2 Under POCAMLA, the Financial Reporting Centre (FRC) is established as the central agency responsible for receiving and analyzing Suspicious Transaction Reports (STRs) as well as dissemination of appropriate information on seizure of criminal proceeds.

2.5.3 POCAMLA identifies Accountants engaged in triggering activities, whether in public practice, or in business together with their practices or employing organizations as "designated non-financial businesses or professions" (DNFBPs). These are certain types of "non-financial" businesses that have been identified as being susceptible to money laundering and terrorist financing due to the nature of their business and the transactions with activity that they may conduct.

2.5.4 Section 48 of POCAMLA places a reporting obligation on Accountants when preparing or carrying out transactions for their clients in the following situations:

- Buying and selling of real estate;
- Managing of client money and securities;
- Management of bank accounts; or
- Creation, operation and management of buying and selling of business entities.

2.5.5 The following are common Money Laundering indicators that Accountants should be aware of (list is not exhaustive):

- Client living beyond their means;
- Client cheques are inconsistent with sale e.g. payments from unlikely sources;
- Client unclear about the location of their premises as well as company records;
- Clients with too few or too many employees inconsistent with the nature of business;
- Unusual payment of consultancy fees to offshore companies as well as sending funds to tax haven jurisdictions;
- Client evading filing of taxes;
- Inconsistencies in company documents that cannot be easily traced in the company records;
- Unusual incoming telegraphic transfers from other companies in foreign jurisdictions when there is no business rationale for such transfers;
- Usage of different auditors and financial advisers for business under the same management and control;
- Clients receiving invoices from organizations with weak AML/TF controls;
- Clients paying extra fees for services which would in normal occasions not warrant such premiums;
- Clients with large account balances, or acquiring high value assets within a short period of being formed;
- Clients providing services and activities not within the normal business operations; and
- Numerous changes in the legal structure of the company (name, location and transfer of ownership and management).

2.6. What is the Prevention of Terrorism Act (POTA)?

2.6.1 Prevention of Terrorism Act (POTA) was enacted on 12th October 2012 to amongst others empower the Financial Reporting Centre (FRC) to fight financing of terrorism. The act outlines offenses associated with terrorism as;

- Possession of property for terrorism;
- Soliciting and supporting terrorist groups;
- Harboring of terrorists;
- Recruitment of people into a terrorist group;
- Provision of weapons to facilitate terrorism;
- Training of terrorists or people to join terrorism group; and
- Obstruction of justice.

2.6.2 The act also gives law enforcers the right to arrest, gather information and seize property associated with terrorism acts as well as subject suspects to a court process.

2.6.3 The accounting profession is diverse varying in the size and sophistication of the firms and its staff, the nature of services offered, and clients served. As part of their day to day operations, accountants provide services that make them vulnerable to become unknowingly involved in MLTF activities. For example, professional money launderers have been known to keep a shadow accounting system with records of transactions involving proceeds of crime.

2.6.4 The accounting sector must meet customer due diligence and record-keeping requirements when, on behalf of their client, they are involved in real estate transactions; managing money, securities or other assets; managing bank, savings or securities accounts; creating, operating or managing companies, or legal persons and arrangements and buying and selling business entities.

2.7. What is the Risk Based Approach (RBA)?

2.7.1 The Risk Based Approach (RBA) is key to satisfying the Kenyan ML/TF regime and FATF recommendations. The RBA is critical to accountants because it relates to their ethical obligations as professionals – to avoid assisting criminals or facilitating criminal activity. It requires organizations to analyze the ML/TF risks they face, make proportionate responses to them, and is the foundation of any business' AML policies, controls and procedures.

2.7.2 Under the FATF Guidance for Accounting Professionals 2019, accountants should identify, assess and understand the ML/TF risks to which they are exposed

and take the required anti-ML/TF measures to effectively and efficiently mitigate and manage the risks.

2.7.3 For accountants, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions in which they operate and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training.

2.7.4 The RBA is not a "zero failure" approach; there may be occasions where an accountancy practice has taken reasonable and proportionate Anti-ML/TF measures to identify and mitigate risks but is still used for ML/TF purposes in isolated instances.

2.7.5 Key elements of an RBA can be summarized as follows:

- ***Risk identification and assessment*** - Identifying ML/TF risks facing an institution, given its clients, services, countries of operation, also having regard to publicly available information regarding ML/TF risks and typologies. This should be performed as part of the overall client and engagement acceptance or continuance processes. The assessments should be documented, kept up to date, and have appropriate mechanisms to provide risk assessment information to authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations;
- ***Risk management and mitigation*** - Identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks;
- ***Ongoing monitoring*** - Putting in place policies, procedures and information systems to monitor changes to ML/TF risks; and
- ***Documentation*** - Documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks.

2.7.6 Senior management is responsible for managing all of the risks faced by the institution, including ML/TF risks. Senior managers should ensure that ML/TF risks are analyzed, and their nature and severity identified and assessed, in order to produce a risk profile. Senior management should then act to mitigate those risks in proportion to the severity of the threats they pose.

2.7.7 The risk analysis can be conducted by the MLRO but must be approved by senior management including the senior manager responsible for compliance (if a different person to the MLRO). This is likely to include formal ratification of the outcomes, including the resulting policies and procedures, but may also include close senior management involvement in some or all of the analysis itself.

2.7.8 An institution with a simple client base and a limited portfolio of services may have a simple risk profile. In which case, a single set of AML policies, controls and procedures may suffice across its operations. Many Businesses will find that their risk analysis reveals different ML/TF risks in different aspects of the business. Various accountancy services such as systems auditing, accounting, taxation and public finance management, for example, may face significantly different risks. A risk analysis allows resources to be targeted, and procedures tailored, to address those differences properly.

2.7.9 Risk Assessment: ML/TF risks can be organized into three categories - country or geographic risk; client risk; and transaction or service and associated delivery channel risk. Below is an overview of the different types of risks and how they can be assessed. See further guidance under 9.1 Guidance to implementing a Risk Based Approach.

(a) Country/Geographic risk:

A client may be at a higher risk when features of his/her business are connected to a higher risk country as regards:

- The origin, or current location of the source of wealth or funds;
- Where the services are provided;
- The client's country of incorporation or domicile;
- The location of the client's major operations;
- The beneficial owner's country of domicile; or
- Target company's country of incorporation and location of major operations (for potential acquisitions).

Higher risk countries may be considered as those that are specifically identified by credible sources:

- To be providing funding or support for terrorist activities or that have designated terrorist organizations operating within them;
- To be having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling;

- To be subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations;
- To be having weak governance, law enforcement, and regulatory regimes, including countries identified as having weak AML/CFT regimes; or
- To be uncooperative in providing beneficial ownership information to competent authorities.

(b) Client risk

dered are:

- The client base includes industries or sectors where opportunities for ML/TF are particularly prevalent;
- The firm's clients include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients;
- Clients where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owner or controlling interests;
- Clients that are cash (and/or cash equivalent) intensive businesses;
- Charities and other "not for profit" organizations that are not subject to monitoring or supervision by designated competent authorities;
- Clients using financial intermediaries, financial institutions or other professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities;
- Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for a proper risk assessment to be performed;
- Clients who have no address, or multiple addresses without legitimate reasons;
- Clients who have funds that are obviously and inexplicably disproportionate to their circumstances such as their age, income, occupation or wealth;
- Clients with previous convictions for crimes that generated proceeds, who instruct Accountants (who in turn have knowledge of such convictions) to undertake specified activities on their behalf; or
- Clients who change their settlement or execution instructions without appropriate explanation.

(c) Transaction/Service and associated delivery channel risk

An overall risk assessment should also include determining the potential risks presented by the services offered, noting that various Accountants provide a broad and diverse range of services. Such services may give rise to suspicious money laundering activity.

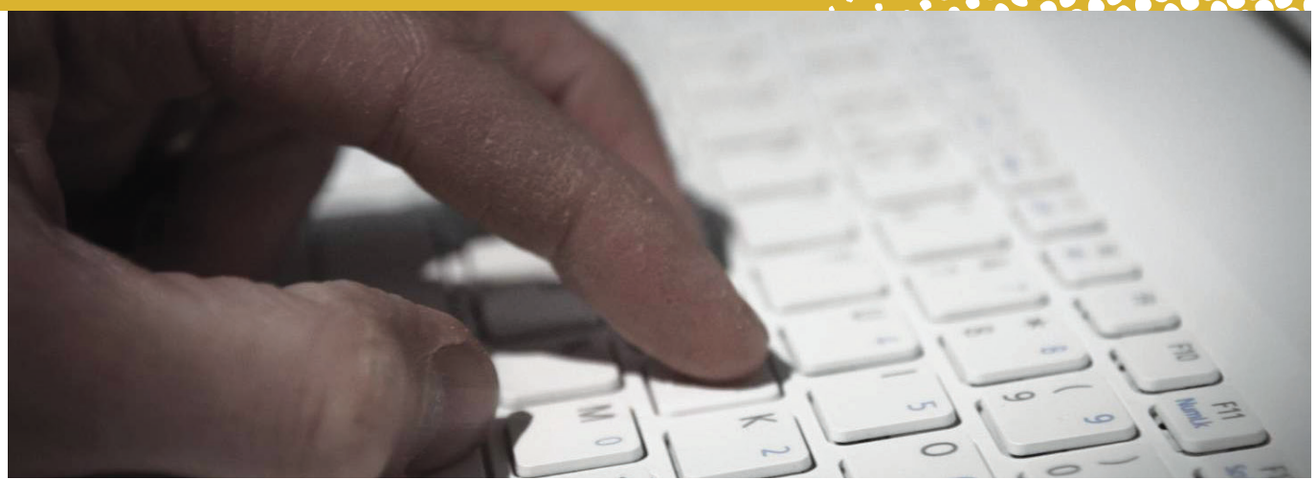
2.7.10 In relation to the areas of risk identified above, also consider the examples of fraud risk factors listed in International Standard of Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240) and the examples of conditions and events that may indicate risks of material misstatement in International Standard of Auditing 315: Identifying and assessing risks of material misstatement through understanding the entity and its environment (ISA315). Even where the accountant is not performing an audit, ISA 240 and ISA 315 provide helpful lists of additional red flags.

2.7.11 Risk Based Approach Challenges for Accountants:

- Implementation - Implementing a RBA can present a number of challenges in identifying what necessary measures they need to take. A RBA is reliant on individuals exercising sound and well-trained judgement when designing and implementing such policies and procedures.
- Sound judgement – One needs to have a good understanding of the risks and should be able to exercise sound judgement. This requires the profession, and the individuals within it, to build expertise through practice and training. If one attempts to adopt a RBA without sufficient expertise, or understanding and knowledge of the risks faced by the sector, they may make flawed judgements. A reviewer may overestimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, and thereby create vulnerabilities.
- Access to information - Developing sound judgement needs good information, and intelligence sharing by designated competent authorities. The existence of good practice guidance, training, industry studies and other available information and materials will also assist the one to develop methods to analyze the information in order to obtain risk based criteria. This information and guidance should be easily accessible so that users have the best possible knowledge on which to base their judgements.

- Risk of criminality – Due to their crucial role in providing a legally required window into the financial health and operations of a firm, Accountants should be particularly alert to ML/TF risks posed by the services they provide to avoid the possibility that they may unwittingly commit or become an accessory to the commission of a substantive offence of ML/TF.

- Accountants must be able to demonstrate to their anti-money laundering supervisory authority how they assess and seek to mitigate ML/TF risks. This assessment must be documented, and made available to the anti-money laundering supervisory authority on request. The documentation should demonstrate how the risk assessment informs their policies and procedures.



3 Obligations and Supervision

- What are the obligations of practitioners and audit firms?
- Approval requirements for the Board and Senior Management
- What is the Money Laundering Reporting Officers (MLRO) role?
- What internal controls should Institutions implement?
- Auditors report on financial statements
- What controls and obligations does ICPAK have with respect to its members and member firms?
- Penalties for non-compliance

3.1. What are the obligations of practitioners and audit firms?

3.1.1 The POCAMLA Regulations require that institutions shall implement anti-money laundering systems and controls that meet the requirements of the Kenya anti-money laundering regime. The Regulations impose a duty to ensure that employees are kept aware of these systems and controls and are trained to apply them properly (see Section Seven of this Guidance).

3.1.2 Institutions are explicitly required to (See Part III of the Regulations):

- Undertake a Money Laundering Risk Assessment;
- Develop and implement Board approved policies that will enable it to effectively manage and mitigate the identified risks;
- Put in place procedures and mechanisms for monitoring implementation of the controls and enhance them, where necessary;
- Update its risk assessment policies or programs regularly but at least once every two years taking into account changes such as the entry of the institution into new markets and the introduction of new products and services; and
- Take reasonable measures to prevent the use of new technologies for money laundering purposes. Such measures include conducting a money laundering risk assessment prior to the introduction of a new product, new business practice or new technology for both new and pre-existing products; so as to assess money laundering risks in relation to a new product and a new business practice, including a new delivery mechanism and new or developing technologies for both new and preexisting products.

3.1.3 The POCAMLA Act places the following additional obligations for Institutions:

- Internal reporting procedures (See Section 3.4 of this Guideline)
- Verification of customer identity (See Section Four of this Guideline);
- Enhanced Customer Due Diligence and countermeasures for higher risk countries (See Section Four of the Guideline);
- Monitoring and Reporting (See Section Five of this Guideline);
- Appropriate record keeping (See Section Six of this Guideline);

3.1.4 Where an Institution fails to meet its obligations under the POCAMLA Regulations and Act, with the consent or connivance of any director, manager, secretary or any other officer of the Institution, or any person purporting to act in such capacity, that person, as well as the Institution, shall be prosecuted in accordance with the provisions of POCAMLA. Such persons are in

addition thereto, liable to both civil monetary penalties and administrative action. Individuals can also be held personally liable for their actions.

3.1.5 Given its size, governance structure and nature of business, a sole practitioner need not:

- Appoint a board member to be responsible for the firm's compliance with POCAMLA, as the practitioner will be held responsible;
- Appoint a MLRO because the practitioner will be responsible for submitting external reports to the Centre; and
- Establish an independent audit function for AML policies, controls and procedures.

3.1.6 In accordance with the international code of ethics for accountants, it is the professional duty of an accountant to maintain the confidentiality of client information. However, the duty of confidentiality may be overridden by statute, the law or courts of law. It is stipulated in section 17 of the POCAMLA that the provisions of the Act shall have effect, notwithstanding any obligation as to secrecy or other restrictions. Section 17 of the POCAMLA therefore overrides professional confidentiality of accountants to make communications to law enforcement authorities.

3.2. Approval requirements for the Board and Senior Management

3.2.1 The approval of Senior Management must be obtained:

- For the policies, controls and procedures adopted by the business.; and
- Before entering into or continuing a business relationship with a Politically Exposed Person (PEP), a family member of a PEP or a known close associate of a PEP or a Prominent Influential Person (PIP).

3.2.2 Such Senior Management staff should receive Continuous Professional Development (CPD) appropriate for the role.

3.2.3 Where appropriate to the size and nature of the business, a board member or member of senior management should be appointed to be responsible for compliance with the anti-money laundering regulations.

3.3. What is the Money Laundering Reporting Officers (MLRO) role?

3.3.1 The Money Laundering Reporting Officer (MLRO) shall ensure;

- S/he is informed of all suspicious activities available to the reporting institution and take action on suspicious disclosures from officers and employees of the institution as soon as practical so as not to delay the reporting of such disclosures;
- Where a disclosure is made, s/he applies internal risk management procedures on a suspicious transaction;
- S/he reports disclosures deemed suspicious to the Financial Reporting Centre as prescribed.
- Officers and employees of the institution are made aware of POCAMLA as well as the audit systems adopted by the reporting institution; and
- In liaison with the institution's human resource department, persons are screened before being hired as employees.

3.3.2 The appointment or removal of the Money Laundering Reporting Officer shall be communicated in writing to the Financial Reporting Centre and the supervisory body ICPAK, within fourteen days of the appointment or removal as per the POCAMLA Regulations, 2013 Section 10 (7).

3.3.3 An Internal Auditor and a Chief Executive shall not qualify to be appointed as a Money Laundering Reporting Officer except in the circumstances where the Chief Executive is a sole practitioner.

3.3.4 Regulation 10 (2) of the POCAMLA Regulations requires that the MLRO should be of management level and have relevant and necessary authority and independence.

3.4. What internal controls should an Institution implement?

3.4.1 The reporting institutions shall formulate, adopt and implement internal control measures and other procedures to combat money laundering. These measures include:

- Adopting an independent audit function to check compliance by the institution with the Act and Regulation (This does not apply to sole practitioners – See 3.1.5);
- Programmes for assessing risks relating to money laundering;
- The formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow-up;
- Monitoring Programmes in relation to complex, unusual or large transactions or suspicious activities;

- Enhanced due diligence procedures with respect to persons and business relations and transactions carrying high risk and with persons established in jurisdictions that do not have adequate systems in place to combat money laundering;
- Providing employees, including the Money Laundering Reporting Officer, from time to time, with training to facilitate recognition and handling of suspicious transactions;
- Making employees aware of the procedures under the Act, these Regulations or directives, codes and guidelines issued thereunder or and any other relevant policies that is adopted by the reporting institution;
- Providing for the necessary processes and working methods including a manual of compliance procedures to ensure adherence to the Proceeds of Crime and Anti-Money Laundering Act; and
- Provide for the responsibility of the management of the reporting institution in respect of compliance with the Proceeds and Crime and Anti-Money Laundering Act.

3.4.2 Employees must be aware of the broad policy and the established ML/TF risk identification and reporting procedures, and the controls must be applied consistently. Controls should also be in place to prevent unauthorized disclosures of monitoring orders.

3.5. Auditors report on financial statements

3.5.1 Where it is suspected that money laundering has occurred, the auditor will need to apply the concept of materiality when considering whether the auditor's report on the financial statements need to be modified, taking into account whether:

- The crime itself has a material effect on the financial statements;
- The consequences of the crime have a material effect on the financial statements; or
- The outcome of any subsequent investigation by the police or other investigatory body may have a material effect on the financial statements.

3.5.2 The concept of materiality should also consider materiality for Terrorist Financing purposes given that the sums may be low value but have a high impact. In addition, the concept should not be restricted to financial statements but should also look at other factors or effects it may have on the organization.

3.5.3 If it is known that money laundering has occurred and that directors or senior employees of the firm were knowingly involved, the auditor will need to consider whether the auditor's report is likely to include a modified opinion on the financial statements. In such circumstances, the auditor considers whether disclosure in the report on the financial statements, either through qualifying the opinion or referring to fundamental uncertainty, could alert a money launderer and constitute a tip-off.

3.5.4 Timing may be the crucial factor. Any delay in issuing the audit report pending the outcome of an investigation is likely to be impracticable and could in itself alert a money launderer. The auditor should seek advice from the MLRO who acts as the main source of guidance and if necessary is the liaison point for communication with the FRC.

3.5.5 The auditor may resign from the position as auditor if he believes that the client or an employee is engaged in money laundering or any other illegal act, particularly, where a normal relationship of trust can no longer be maintained.

3.5.6 Where the auditor intends to cease to hold office there may be a conflict between the requirements under the Companies Act for the auditor to deposit a statement at a company's registered office of any circumstances that the auditor believes need to be brought to the attention of members or creditors and the risk of 'tipping off'. This may arise if, for example, the circumstances connected with the resignation of the auditor include knowledge or suspicion of money laundering and an internal or external disclosure being made.

3.5.7 Where such disclosure of circumstance may amount to 'tipping off', the auditor should preferably seek advice from the MLRO who acts as the main source of guidance and if necessary is the liaison point for communication with lawyers, the FRC and the relevant law enforcement agency.

3.5.8 Where the only information which needs to be disclosed is the underlying circumstances which gave rise to the disclosure, there are two scenarios to consider:

- Where the auditor only wishes to disclose the suspicions about the underlying criminal conduct and the basis for those suspicions, the auditor will not commit an offence under POCAMLA if that information only is disclosed. For example, if audit files are made available to the incoming auditor containing working papers that detail circumstances which have led the audit team

to suspect the management of a fraud and this suspicion is noted on the file, this will not constitute a 'tipping off' offence; or

- If the auditor wishes to disclose any suspicions specifically about money laundering (for example, if the working papers in the example above indicated that the suspected fraud also constituted a suspicion of money laundering), then as a matter of prudence, reporting should follow procedure indicated in the POCAMLA.

3.5.9 The offence of 'tipping off' may also cause a conflict with the need to communicate with the prospective successor auditor in accordance with legal and ethical requirements relating to changes in professional appointment. For example, the existing auditor might feel obliged to mention knowledge or suspicion regarding suspected money laundering and any external disclosure made to the FRC.

3.5.10 Although the POCAMLA and its regulations are silent on this, this guide recommends that it would not constitute 'tipping off' if it was done to prevent the incoming auditor from committing a money laundering offence.

3.5.11 Where any information relating to an offence under POCAMLA is received by the FRC or an authorized officer, the information and the identity of the person giving the information shall be kept confidential per Section 20 of POCAMLA on protection of information and informers. Auditors should work with the MLRO to file such information with the FRC. See POCAMLA Section 20 for additional guidance.

3.6. What controls and obligations does ICPAK have?

3.6.1 ICPAK as regulator of the accountancy profession in Kenya has put in place a mechanism for reviews to be undertaken for accountants together with their practices or employing organizations engaged in triggering activities (See 1.3). These reviews are conducted as part of the Audit Quality Reviews (AQR).

3.6.2 The AQR is designed to include the independent testing of money laundering prevention and detection procedures and should be conducted at least once in every three years. The AQR report should be deposited with ICPAK.

3.6.3 ICPAK requires that the AQR is designed to involve interviews with personnel engaged in triggering activities, ethics, risk and compliance staff as well as relevant designated reporting officers within the institutions. AQR tests, among other things, will be conducted in order to assess:

- Customer Due Diligence requirements (see Section Four);
- Maintenance of all AML systems and Transaction Monitoring (See Section Five);
- Record keeping procedures (See Section Six);
- Compliance with monitoring orders;
- Employee training (see Section Seven); and
- Escalations and conflict checks and auditor independence.

3.7. Penalties for non-compliance

3.7.1 Without derogating from any criminal penalty or other sanction that may be imposed by POCAMLA, where an accountant engaged in triggering activities is in breach of, or fails to comply with this guideline, ICPAK may for reasons disclosed in writing:

- Issue a warning to the person or institution;
- Issue an order requiring the person or institution to comply with a specific instruction or direction;
- Issue an order of suspension or revocation of a license, registration, permit or authorization of a specified individual or institution whether entirely or in a specified capacity or of any director, principal, officer, agent or employee of the institution; or
- Refer the person or institution to the Financial Reporting Center for further criminal or administrative action.

3.7.2 Before administering penalties for non-compliance, ICPAK shall give the person or institution a written notice of not less than fourteen days requiring the person or institution to show cause as to why the prescribed action should not be taken. Such actions shall be heard and determined by the Disciplinary Committee as established under the Accountants Act.

4 Customers Due Diligence (CDD)

- Why is CDD important?
- When should CDD be performed?
- Types of CDD
- Politically Exposed Persons
- How should CDD be applied?

Part IV of the POCAMLA Regulations provide for minimum acceptable requirements for a General CDD. This guidance should be read in line with the provisions of the regulations.

4.1. Why is Customer Due Diligence Important?

4.1.1 Recommendation 10, FATF defines Customer Due Diligence (CDD) as the program implemented by institutions to know more about its customers and be able to prevent money laundering abuses. Criminals often seek to hide their true identity by using complex and opaque ownership structures. The purpose of CDD is to know and understand a client's identity and business activities so that any ML/TF risks can be properly managed. See POCAMLA Regulation 12 for objectives of CDD.

4.1.2 Customer Due Diligence is appropriate in any business to verify the natural person (a human being as opposed to a legal person) behind the entity who is the beneficial owner, as well as to verify the information provided by the client. By understanding the client business as well as its normal operations, a business is likely to note when something abnormal is taking place which may act as a red flag to initiate a money laundering investigation.

4.1.3 A beneficial owner in a business structure is defined as a person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted, and any person who ultimately exercises effective control over a legal person or arrangement.

4.2. When should CDD be performed?

4.2.1 A reporting institution shall take measures to satisfy itself as to the true identity of any applicant seeking to enter into a business relationship with it, or to carry out a transaction or series of transactions with it, by requiring the applicant to produce an official record for the purposes of establishing the true identity of the applicant and for the purpose of verifying that identity.

4.2.2 POCAMLA Regulations 12 (2) state that CDD should be done:

- When establishing initial business relations;
- When undertaking occasional or one-off transactions;
- When there is cause to be suspicious; and
- When there is doubt about veracity or adequacy of previously obtained customer information.

4.2.3 At a minimum, a sound CDD program should incorporate measures to:

- Verify a customers' identity using independent sources, documents and data;
- Understand the purpose and nature of his business or principal activity;
- Understand his financial status; and
- Confirm the capacity in which he is entering into the business relationship.

A business relationship refers to an arrangement between a person and a reporting institution, where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the person and the reporting institution on a frequent basis. This is as opposed to one-off transactions, defined in the regulations as any transaction carried out other than in the course of a business relationship.

4.2.4 Main elements of a sound customer due diligence program are as follows:

(a) Customer identification - Full identification of the customer ranging from the source of funds and nature of business. The institution should have procedures to track changes in customer details over time;

(b) Customer profiles - Involves the development of the customer reviews on the anticipated versus actual account activity. Deviation from the expected profile may prompt investigation and subsequently filing of an STR;

(c) Customer acceptance / continuance - The institution gives consent to the applicant to use its products and services depending on the jurisdiction they are in;

(d) Risk rating - Assessing and grading customers depending on the risks they pose after accepting the business relationship. The risk-based approach should be adopted to identify the products/ services, clients and geographical areas that are riskier than others;

(e) Monitoring - Involves continuous account, transaction and advanced media monitoring for any risks.

(f) Investigation - Arises when the institution detects unusual account patterns from what is expected. Deviation from the norm does not necessarily amount to money laundering if the client can prove beyond reasonable doubt that the change is legitimate. For salary accounts for instance, the institution would expect proceeds from salary. If more cash is credited into the account, the account holder may be required to support the pattern with business permits and certificate of registration in case they run a business.

(g) Documentation - This is proof that investigation did happen and findings were maintained. The absence of supporting documentation should imply that no investigation took place.

4.3. Types of CDDs

4.3.1 Standard Due Diligence (SDD) - This is the basic level of know your customer (KYC) checks applied to customers assessed to pose lower money laundering and terrorism financing risk (See Section 2.7 Risk Based Approach). The information obtained from the customer should be verified through credible and independent sources. Standard Due Diligence can be done through:

- Documentary verification – For instance, accomplished by obtaining customers identification details such as name from an Identity card/passport and confirming the physical address through a utility bill or Tax PIN.
- Non-documentary verification – For instance the "Identity Number" (ID number) is verified through a government database such as IPRS (Integrated Population Registration Service) to confirm that the details match with the government records. Call backs through phone/letter or email can be used to confirm details provided during account opening.
- Eligible introducers - Where an applicant for business is introduced by an eligible introducer or a group introducer, it shall be sufficient compliance with POCAMLA Regulations where the reporting institution obtains and maintains documentary evidence that the eligible introducer or group introducer is regulated for the purposes of preventing money laundering; and is satisfied that the procedures laid down by the eligible introducer or group introducer meet the requirements specified in POCAMLA, or any code or guidelines issued by a supervisory authority.

4.3.2 Enhanced Due Diligence (EDD) is a more sophisticated KYC process especially to business partnerships and products assessed to pose a higher money laundering and terrorism financing risk to financial institutions (See Section 2.7 Risk Based Approach). POCAMLA Regulation 18 recommends that EDD can be done through the following measures:

- Obtaining further information that may assist in establishing the customer's identity;
- Applying extra measures to verify the documents supplied;
- Obtaining senior management approval for the new business relationship or transaction
- Establishing the person's or entity's source of funds; and
- Carrying out ongoing monitoring of the business relationship.

4.3.3 Recommendation 10, FATF appreciates the fact that there are scenarios in which ML/TF risks are higher thus requiring additional scrutiny on CDD. Enhanced due diligence is important in scenarios such as below;

Customer Risk	Geographical risks	Product/Service risks
• Foreign customers. • Companies with nominee shareholders or in bearer shares. • Complex company ownership structures. • Cash intensive business as supermarkets and car wash and restaurants. • Customers represented gatekeepers such as lawyers and secretaries. • Sudden change of the client transacting pattern such as large transfers to and from tax havens or high-risk jurisdictions with no apparent reason.	• Countries subject to the United Nations, OFAC, UKHMT and other major sanctions and trade embargoes. • Countries known or suspected to finance Terrorist activities per the UN and US Government lists. • Countries known to have weak MLTF laws as per FATF mutual evaluation reports, EU, UN, USA and other major entities. • Countries noted to be tax havens. • FATF list of high-risk jurisdictions subject to a call for action (black list) and jurisdictions under increased monitoring (grey list).	• Non-face to face business transactions. • Private banking transactions • Payments received from unidentifiable third parties.

4.3.4 Ongoing Due Diligence is recommended after a business relationship has been established. This is important to ensure that the records before inception of the business relationship are consistent with the client's operations.

4.3.5 Circumstances that may prompt one to carry out ongoing due diligence include:

- Event driven reviews as:
  - Changes in business ownership/structure of the client;
  - Client becoming Politically exposed Person (PEP);
  - Suspicion that the client may be engaging in money laundering activities. This should be done carefully without tipping off the client. Whereas tipping off amounts to an offence under POCAMLA, the FATF recommendation 21 do not establish criminal offenses;
  - Client entry into a new business different from what was maintained in the Memorandum of Association;
  - Negative media publicity on the client;
  - At the commencement of new engagements and when planning for recurring engagements; or
  - Where the customer has ventured into business in a high-risk jurisdiction.
- Periodic reviews that are prompted by the risk category of the client. For instance, high risk clients ought to be reviewed yearly, medium risk after two years and low risk customers after a period of three years at a minimum.

4.4. Politically Exposed Persons (PEPs)

4.4.1 Politically Exposed Persons (PEPs) are people who by the nature of their positions in society, pose higher ML/TF risks. POCAMLA Regulations define a PEP as a person who has been entrusted with a prominent public function in a country or jurisdiction (See Section 22 (3)).

4.4.2 The definition includes beneficial owners such as immediate family members or close business associates of the PEP.

4.4.3 Institutions shall have risk management procedures in place to determine whether the customer or beneficial owner is a politically exposed person.

4.4.4 Institutions will be required to take the following measures where a customer or beneficial owner is a politically exposed person. These measures should be documented, and records retained:

- Obtain approval from senior management to transact or establish the relationship with that person;
- Take adequate measures to establish the source of wealth and the source of funds which are involved in the proposed business relationship or transaction;
- Obtain information on the immediate family members or close associates of the person who may be having transaction authority over the account;
- Determine the purpose of the transaction or account and the expected volume and nature of account activity;
- Review public sources of information on the politically exposed person; and

- Once the account has been established, conduct enhanced ongoing monitoring of the

4.4.5 Types of Politically Exposed Persons (PEPs):

- Domestic PEPs - These are individuals who have been entrusted with public functions within their country. They include Heads of state, attorneys general, chief justice, ministers, senior politicians, senior executives of state-owned corporations and officials to major political parties.
- Foreign PEPs - Individuals entrusted with public functions in a foreign country. They include Heads of State, ambassadors, judicial or military officials, senior politicians and government officials.

4.4.6 Recommendation 12, FATF indicates that an individual remains a PEP after a period of 12 months after leaving office or position that made him/her become a PEP. However, the Kenyan law does not specify the period within which a person can remain a PEP after cessation of office.

4.4.7 Prominent Influential Persons (PIPs) - These are individuals that are not necessarily PEPs but either hold, or have held, a prominent public function. For example, senior media personalities, renowned sports individuals, entrepreneurs and musicians.

4.4.8 This guideline recommends that PIPs be accorded the same treatment as PEPs.

4.5. How should CDD be applied?

4.5.1 Customer Due Diligence should be applied as per the Risk-Based Approach (FATF recommendation 1). The Risk-Based Approach (RBA) requires that organizations put in place appropriate systems and controls to prevent money laundering and terrorism financing risks to the lowest level possible.

4.5.2 The RBA is considered the appropriate method in combating MLTF crimes because:

- It is flexible - Money laundering and terrorist financing risks vary across various geographical locations, customers and products over time;
- Proportionate - Noting that there is no fixed definition of suspicion in money laundering, a 'check-the-box' approach is not considered the most appropriate approach; and
- Effectiveness - Institutions are the first contact with their clients. Therefore, institutions are in a better position to identify where their greatest risk lies and put in place controls and systems to mitigate them.

4.5.3 Institutions may categorize MLTF risks into the following levels;

- Prohibited - These are those business or products that a company should not accept any dealings with. This includes transactions or persons from sanctioned countries as listed by the European Union, United Nations or Office of Foreign Asset Control (OFAC). Sanctioned countries are those suspected to sponsor terrorism in monetary terms or producing weapons meant for terrorist activities;
- High-risk - These risks are significant but not necessarily prohibited. Institutions are required to implement controls to mitigate such risks as well as continuous monitoring. These may include transactions from countries prone to corruption and drug trafficking, PEPs, and correspondent banking services;
- Medium risk - These are risks that require scrutiny but do not qualify as high-risk levels. For example, small restaurants that have moderate cash flows and not considered cash intensive; and
- Low risk - These are baseline money laundering risks that indicate normal business operations.

4.5.4 Recommendation 10, FATF recommends that in situations where CDD had delayed, an institution should still identify possible ML/TF risk posed by a client. Completion of CDD can be done when the relationship has been established on condition that the risk is low to avoid interruptions in normal operations of the client. The client should be ready to provide the information within the specified timelines as too much delay may give rise to suspicion.

4.5.5 Client engagements as transfer of assets must only be commenced after completion of CDD.

5 Suspicious Transaction Reports (STR)

- The reporting regime
- What must be reported?
- What are the reporting procedures?
- Follow up – what happens after reporting?

5.1. The reporting regime

5.1.1 Section 2 of POCAMLA Regulations includes Accountants as reporting institutions and as such, are expected to file external reports with the FRC.

5.1.2 An internal reporting procedure that enables employees to report their knowledge or suspicions of MLTF should be in place. An MLRO must be appointed to receive these reports (See section 3.3).

5.1.3 It is an offence for someone who knows or suspects that MLTF has occurred (or has reasonable grounds to do so) not to report their concerns to their MLRO (or, in exceptional circumstances, directly to the FRC).

5.1.4 The MLRO has a duty to consider all such internal STRs and, if the MLRO also suspects MLTF, then an external report must be filed to the FRC.

5.1.5 While there is no definitive guidance on what constitutes 'suspicion' with regard to ML, what one is looking for is an indication that funds or assets that are the subject of a transaction came into the customer's hands as a result of illegal activity. In the case of TF, one is looking for an indication that the transaction is connected in some way with a terrorist, a terrorist group, or an act (planned or past) of terrorism.

5.1.6 A suspicious transaction is one that raises questions or gives rise to discomfort, apprehension or mistrust – even without sufficient evidence. Note that the term 'transaction' includes completed, proposed or attempted transactions.

5.1.7 Suspicion is not mere idle wondering, a vague feeling of unease or a lack of understanding whether due to insufficient knowledge, ignorance, naivety or ineffective due diligence on the part of the employee or reporting institution.

5.1.8 MLROs should guard against making speculative Suspicious Transaction Reports (STRs) – STRs should be filed where observed behavior/transactions is not in line with behavior/transactions expected of a reasonable person, business or account in the same position. For example, the purchase of a high-end property by a client's financial controller is not, in itself, suspicious activity. However, inconsistencies in accounts for which the financial controller is responsible could raise speculation to the level of suspicion.

5.1.9 Accountants are in a position to discover ML/TF because of their expertise and involvement in execution and facilitation of a wide range accountancy services (See section 2.2). A list of sector specific MLTF indicators is available under section 2.5.5.

5.2. What must be reported?

5.2.1 A reporting institution shall file suspicious transaction reports and cash transaction reports, as required, to the Financial Reporting Centre. Suspicious transaction reports (STR) apply where suspicious activity is identified whilst cash transaction reports (CTR) apply to all cash transactions that exceed USD 10,000, whether suspicious or not. All reporting institutions must also submit an Annual Compliance Report (ACR).

5.2.2 Suspicious Transaction Reports - STRs must be filed immediately and within seven days of the date of the transaction or occurrence of the activity that is considered suspicious. Sufficient information such as the nature of and reason for the suspicion must be disclosed. Where additional supporting documentation is available, these should be provided. The Suspicious Transaction Report shall be in the form prescribed by the Financial Reporting Centre and the FRC will acknowledge receipt of the report.

5.2.3 Cash Transaction Reports - CTRs must be filed on all cash transactions equivalent to or exceeding US$ 10,000 or its equivalent in any other currency, whether or not the transaction appears to be suspicious. CTRs must be made electronically, by Friday in the week in which the transaction occurred. The FRC will acknowledge receipt of the report.

5.2.4 Annual Compliance Report - The Proceeds of Crime and Anti-Money Laundering Regulations require reporting institutions to submit to the Financial Reporting Centre a report indicating the institutions level of compliance with POCAMLA Act, Regulations and the institution's internal anti-money laundering rules. The report is submitted by 31 January of the following year unless the date is varied in writing by the FRC. The FRC circulates an ACR Template towards the end of the year which institutions use for reporting compliance in the ending year. The report may vary from year to year and institutions are encouraged not to submit their reports using templates not intended for the particular year. The ACR templates and corresponding circulars can be downloaded from the FRC's website (http://frc.go.ke/reporting/annual-compliance.html).

5.3. What are the reporting procedures?

Internal procedures

5.3.1 Accountants in employment when reporting suspicious transactions should follow procedures developed by their respective employers; and if no such procedures exist they should advise their employers to put in place reporting procedures and appoint an MLRO for reporting suspicious transactions and any other money laundering activities.

5.3.2 Firms should put in place internal reporting procedures. Such internal procedures should clearly set out what is expected of individuals who discover suspicions or obtain knowledge of possible money laundering. The MLRO is responsible for making decisions on whether the information contained in the suspicious transactions needs to be relayed to the FRC.

5.3.3 It is recommended under this guideline that all details of internal reports of suspicious activity be held by the MLRO and excluded from client files. Exclusion of information from client files assists in avoiding inappropriate disclosure of information and protects against the risk of tipping off. Client files should retain only that information relevant to and required for the professional work being undertaken.

5.3.4 Tipping off offence may be committed if a person knowing or suspecting that a report has been made either to an MLRO or to the FRC, and making any disclosure which he knows or suspects is likely to prejudice any investigation that might follow that report. Section 8 of Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009 prohibits disclosure to unauthorized third parties the fact that a suspicious transaction report or related information is being reported to the FRC.

External procedures – FRC STR reporting guide

5.3.5 The FRC has developed an Excel based STR reporting template called FRC STR Template.xlsm and available on the FRC website (http://frc.go.ke). This is the template to be filled and emailed to FRC to report an STR.

5.3.6 The template can be obtained by registering with the FRC (A reporting institution that is registered with the FRC will obtain the template through its registered email address as part of the confirmation of registration) and requesting the FRC (A reporting institution can request for the template in writing either through email or a letter). The template will be sent to the email address provided in the request.

5.3.7 To file the STR template:

- Make a copy of the STR template keeping the original intact for future use. All other operations below are on the copy not the original;
- Open the STR template in Microsoft Office Excel 2007 and above;

- Excel may display a security warning at the top ribbon stating that some active content has been disabled. Ensure that active content is enabled;
- Proceed and fill in all the relevant sections of the template; and
- Save the template using the following suggested name pattern:STR-YYYY-999- [Reporting Institution] where YYYY is the year, 999 is a sequential number beginning with 001 every calendar year, and reporting institution is the name of your institution. For example, if Audit Firm X is submitting their 11th STR report the year 2020, the name of the report will be "STR-2020-011-Audit Firm X.xlsm"

5.3.8 To submit a completed STR:

- Print, sign, and stamp the filled in report. The template has been set to print properly on A4 paper;
- Scan the signed and stamped report and save is as a pdf file with the same name as the Excel file such as. "STR-2020-011-Audit Firm X.pdf";
- Scan any other additional information to be submitted with the STR;
- Attach the Excel and PDF files and any additional information in one email and email to the provided email address. The subject of the email is to be the same as the name of the files for instance "STR-2020-011-Audit Firm X".

5.4. Follow up – What happens after reporting?

5.4.1 With respect to client relationships:

- After a STR has been submitted the transaction need not stop unless FRC instructs so.
- Even when the FRC has not explicitly instructed that a transaction should be stopped, the institution may wish to consider whether the suspicion is such that for professional or commercial reasons, it no longer wishes to act for a client or his close associates.

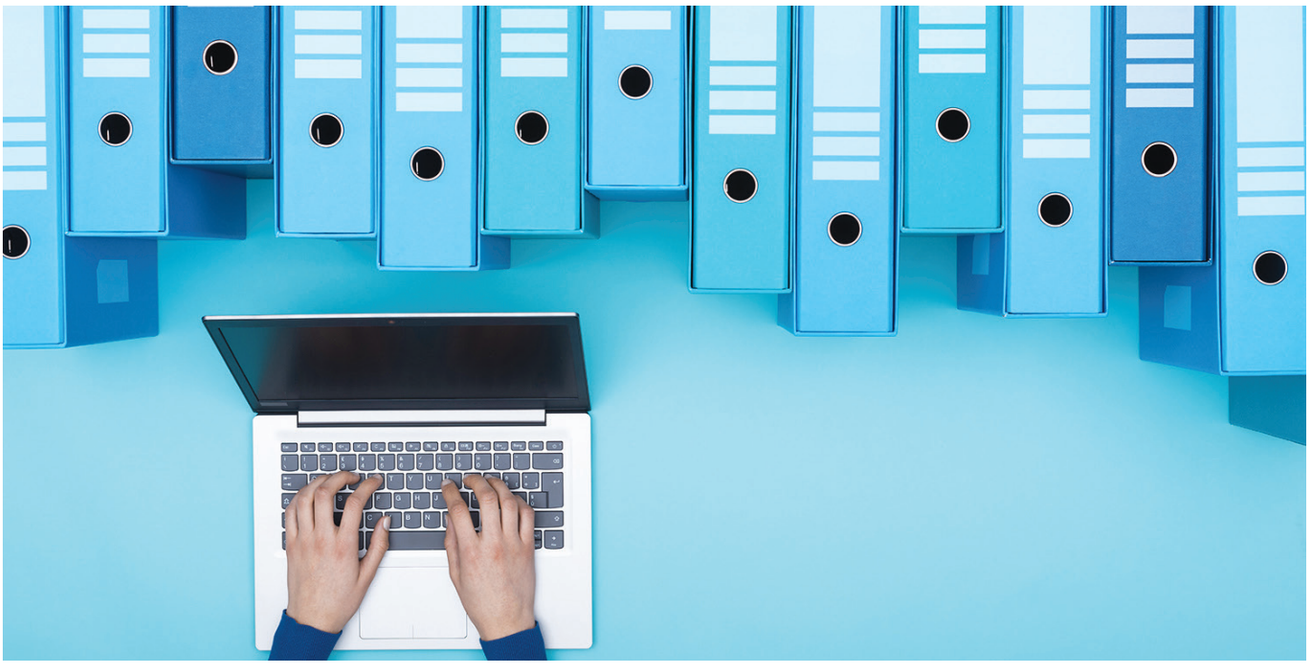
5.4.2 With respect to data protection:

- Personal data that relates to knowledge or suspicion of MLTF (that is, data that has been processed to help prevent or detect crime) need not be disclosed under a subject access request if to do so could constitute tipping off.
- Note that data exempt from one subject access request may no longer be exempt at the time of a subsequent request. It is recommended that the MLRO should be involved in these discussions and the thinking behind any decision to grant or refuse access is documented.

5.4.3 With respect to requests for further information:

- The FRC or other law enforcement authority may seek further information about a SAR. Such information should be provided in full and in a timely manner.
- Before providing such information, it is important to formally verify the enquirer's identity, the authority under which the request is made, timelines and format in which the information is to be provided and what part of the information can be excluded (if any).

5.4.4 Following the filing of STR/SARs, employees must not comment on or provide information to third parties such as members of the press or other employees who need not be aware of the report. All communication must be through the MLRO, who in turn, should consult the Legal Counsel (if any) before providing additional information with regards to a report. Note that under Section 8 of POCAMLA, tipping off is a criminal offence.



6 Record Keeping

- How should records be managed?
- Which records should be maintained?
- What considerations apply to SAR/STR and consent requests
- Managing training records
- Managing Third party arrangements
- Managing personal data

6.1. How should records be managed?

6.1.1 Records of all transactions and evidence obtained as part of CDD checks (or information that would enable copies of such evidence to be obtained) shall be retained.

6.1.2 Such records shall be retained for a minimum of seven years from the date the business or transaction was completed or following the termination of an account or business relationship. An institution would not be liable in an event that an investigation by law enforcement bodies commenced after records are destroyed as per the documented destruction policies. However, it would be an offence if records are destroyed after commencement of investigation even if no warrant had been issued.

6.1.3 The Act and Regulations do not specify the location or format in which records should be stored, but they must be available on a timely basis.

6.2. Which records should be maintained?

6.2.1 The records shall contain sufficient particulars to identify:

- The name, physical and postal address and occupation (or where appropriate business or principal activity) of each person conducting the transaction or on whose behalf the transaction is being conducted, as well as the method used by the reporting institution to verify the identity of that person;
- The nature, time and date of the transaction;
- The type and amount of currency involved;
- The type and identifying number of any account with the reporting institution involved in the transaction;
- If the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsements appearing on the instrument; and
- The name and address of the reporting institution and of the officer, employee or agent of the reporting institution who prepared the record.

6.2.2 Accountants shall take reasonable measures to establish the true identity of an applicant seeking to enter a business relationship. Such measures shall include requiring the applicant to produce original and/or certified copies of official records such as:

- For individuals – a national identity card, a birth certificate, a passport, KRA pin, a driver's license or any other official means as may be prescribed for identification.
- For corporates - a certificate of registration or incorporation, an act establishing the corporate body, the latest annual returns and a corporate resolution authorizing a person to act on behalf of the corporate, and any other items as may be prescribed.
- In cases of a governmental department, a letter from the accounting officer shall be necessary.

6.3. What considerations apply to SAR/ STR and consent requests?

6.3.1 The Regulations (Section 32 (1) requires that upon identification of risk, an institution must report to the FRC within 7 days.

6.3.2 The records relating to filing of an STR/SAR should not be stored together with the regular client records. This is to avoid the risk of inadvertent disclosure or tipping off, which is an offense under Section 8 of POCAMLA.

6.3.3 No retention period is officially specified for records relating to internal reports, the MLRO's consideration of internal reports, any subsequent reporting decisions, issues connected to consent, production of documents and similar matters, suspicious activity reports and consent requests sent to the FRC, or its responses. Further, no period has been specified on retention of STR/SAR. However, since these records can form the basis of a defense against accusations of ML/TF and related offences, institutions may decide that seven years is a suitable retention period for them.

6.3.4 Also note that STR/SARs may arise out of investigations by law enforcement and other bodies. Scenarios that may lead to the commencement of such investigations include:

- Adverse media information;
- Whistleblower reports;
- Escalations from customer facing employees such as tellers, on suspicious behaviors. These may include threats and attempted blackmail by customers;
- Red flags from scenarios and rules in transaction monitoring systems;
- Regulatory recommendations from official government bodies such as in tax evasion cases. or
- Receipt of law enforcement search warrant. Where a search warrant has been issued, an institution should confirm the authenticity of the warrant, understand its scope, obtain a copy of the warrant, inform the financial institution legal counsel of the warrant, request for a copy of the affidavit, take down the names of the officials undertaking the search and take note of the items that have been seized.

6.4. Managing training records

6.4.1 The POCAMLA regulations, 2013 require that all employees including the Money Laundering Reporting Officer, will be provided with training to facilitate recognition and handling of suspicious transactions (see Section seven of this guidance).

6.4.2 Records on such training should clearly identify the employees to be trained, the content of the training, how, when and where to train.

6.4.3 No period has been specified on retention of training records. However, since these records can form the basis of a defense against accusations of ML/TF and related offences, institutions may decide that seven years is a suitable retention period for them.

6.5. Managing third party arrangements

6.5.1 Third parties refer to financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs) or a person supervised or monitored by a competent authority.

6.5.2 Institutions are permitted to get into written agreements with third parties, to execute CDD on their behalf, provided that:

- Such agreements will specify the responsibilities of each party;
- Institutions can adequately satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements, will be made available from the third party upon request in an appropriate format and without delay;
- The institution can ascertain the risk level of the country where the third party is situated; and

- The institution is certain that the third party is regulated, supervised or monitored by a competent authority and has measures in place for compliance with, customer due diligence and record-keeping requirements in line with international best practice such as FATF recommendation 10 and 11. FATF recommendation 10 on CDD, requires that at a minimum, such information shall be sufficient to enable the institution to:
  - Verify the authenticity of customer details from independent and reliable sources;
  - Properly identify the beneficial owner of a corporate body; and
  - Identify the proper intention of the business relationship of a corporate body.

6.5.3 No period has been specified on retention of third-party agreements and records. However, since these records can form the basis of a defense against accusations of ML/TF and related offences, institutions may decide that seven years is a suitable retention period for them.

6.6. Managing personal data

6.6.1 The Kenya Data Protection Act 2019, (Section 39(1) and (2) require that once the retention period has expired, personal data shall be deleted, erased, anonymized or pseudonymized unless such data retention is:

- Required or authorized by law;
- Reasonably necessary for a lawful purpose;
- Authorized or consented by the data subject; or
- Required for historical, statistical, journalistic literature and art or research purposes.

6.6.2 The business is not required to keep any records for more than seven (7) years after the end of the business relationship.

7 Training

- Responsibility
- Content
- Timelines

7.1. Responsibility

7.1.1 The POCAMLA regulations, 2013 require that all employees including the Money Laundering Reporting Officer, will be provided with training to facilitate recognition and handling of suspicious transactions (see Section Five of this guidance).

7.1.2 Training can be delivered in multiple ways including in-person, online training, instructor-led or self-paced study, video presentations, or a combination of all of these.

7.1.3 MLROs and members of senior management may require supplementary training in a customized manner.

7.1.4 A specific person such as the MLRO or a member of senior management should be made responsible for the detail of training.

7.2. Content

7.2.1 The training programme should include:

- The entity's anti-money laundering reporting policy and procedure;
- A description of the nature and processes of money laundering including 'red flags' which employees should be aware covering all aspects of AML procedures;
- An explanation of the underlying legal obligations of both the employee and employer under the anti-money laundering law and guidelines;
- An explanation of the existing systems to prevent and detect money laundering with particular emphasis on the recognition of suspicious transactions and the submission of internal suspicious transaction reports to the MLRO in a timely manner; and
- The relevant data protection requirements.

7.2.2 Content should be customized so that employees are able to use a risk based approach (see Section 2.7 of this guidance) to decide, on a case-by-case basis, the most appropriate approach to take.

7.2.3 Records should be kept showing who has received training, the nature of training received and when training took place (see Section 6 of this guidance). In addition, procedures should be implemented to determine the effectiveness of training.

7.3. Timelines

7.3.1 The regulations require that employees, including the Money Laundering Reporting Officer are provided with training, from time to time, to facilitate recognition and handling of suspicious transactions.

7.3.2 Institutions need to make sure that employees are trained promptly. The frequency of such training can be influenced by multiple factors such as when an employee is on-boarded, change or roles, change of service lines, launching of new product lines or service channels, changes in legislation, regulation, case law and judicial findings.

7.3.3 While it may be unnecessary to repeat whole training programs periodically, it may be appropriate to provide employees with regular updates to help refresh and expand their knowledge and to remind them of emerging risks and new approaches to effective anti-money laundering work. Businesses are also encouraged to undertake periodic awareness campaigns to keep employees alert to individual and institution-wide responsibilities.

7.3.4 The overall objective of training is not for employees to become specialist financial crime control experts. However, they should be well equipped to apply legal and business knowledge reasonably expected of someone in their role and with their experience when deciding whether to make an internal report to the MLRO.

8 Regulatory Examination

- Powers of the Financial Reporting Centre (FRC)
- How to prepare for and what to expect during regulatory examination
- Follow up – What happens after reporting?

8.1. Powers of the Financial Reporting Centre

8.1.1 The Financial Reporting Centre may, at any time, cause an inspection to be made of any reporting institution pursuant to the requirements of the Act and will require that the reporting institution concerned shall produce and make available information sought by the inspector.

8.1.2 Failure to produce information within the period specified shall constitute an offence under POCAMLA.

8.1.3 The information required to be produced shall not, in the course of inspection, be removed from the premises of the reporting institution or other premises at which they are produced.

8.1.4 The Financial Reporting Centre may take administrative and civil action against individuals and institutions for non-compliance with any instruction, direction or rules issued by the Centre.

8.1.5 Before taking administrative action or imposing civil penalties against any person or institution, the Centre shall give the person or institution a written notice of not less than fourteen days requiring the person or institution to show cause as to why the prescribed administrative action should not be taken.

8.1.6 Administrative action may include:

(a) For individuals:

- A warning or order requiring compliance with any specific instruction;
- An order barring an individual or individuals from employment within the specified reporting institution whether entirely or in a specified capacity; or
- An order to a competent supervisory authority requesting the suspension or revocation of a license, registration, permit or authorization of any director, principal, officer, agent or employee of the reporting institution.

(b) For institutions:

- A warning or order requiring compliance with any specific instruction; or
- An order to a competent supervisory authority requesting the suspension or revocation of a license, registration, permit or authorization of a specified reporting institution whether entirely or in a specified capacity.

8.1.7 Civil penalties may include:

(a) For individuals:

- A monetary penalty not exceeding five million shillings; and
- In the case of continued failure, the person shall be liable to an additional monetary

penalty of ten thousand shillings per day on which such failure continues for a maximum period of one hundred and eighty days.

(b) For institutions:

- A monetary penalty not exceeding twenty-five million shillings; and
- In the case of continued failure, the reporting institution shall be liable to an additional monetary penalty of ten thousand shillings per day on which such failure continues for a maximum period of one hundred and eighty days.

8.2. How to prepare for and what to expect during regulatory examination

8.2.1 After notification of an upcoming examination, an FRC Officer will call the MLRO and explain the process. A notification letter with details of the documentation that the FRC will require will then be sent shortly after the initial conversation. If uncertain of any requirements or process, do not hesitate to ask the FRC Officer conducting the examination.

8.2.2 To prepare for an examination:

- Assemble all compliance documentation such as policies and procedures;
- Review all past interactions with FRC;
- Ensure that all relevant staff are available to answer any questions;
- Set a private room for the examiners if the FRC Officer confirms that they are coming to the premises;
- Observe the deadlines noted in the letter from FRC Officer;
- Provide all documents and transactions listed in the letter; and
- Answer all questions honestly and have resources available on hand during the examination.

8.2.3 The following is a summary of what to expect as part of the examination process:

- Notification of the examination – A call or letter from the Centre notifying you that they will be conducting an examination;
- Information request – A letter requesting specific information and timelines by which such information should be provided. The letter will also indicate the date that the exam will start;
- Kick-off meeting and the Examination – The FRC Officer will meet all relevant staff and introduce the Centre's team and make any clarifications needed. The FRC officer will ask questions and request for documents relevant to the examination. The questions will cover various aspects of your organization including general business information, management structures and internal controls, AML policies and procedures, risk assessment, training programs and record keeping practices;
- Exit meeting – A summary of deficiencies noted from the exam will be provided. Any questions arising from deficiencies should be asked at this time including obtaining suggestions on how best to remedy all deficiencies. The Officer may also give an indication of when a formal letter with the deficiencies will be sent to you.

8.3. Follow up – What happens after an examination?

8.3.1 Expect to receive a letter from the Centre summarizing all deficiencies noted during the examination.

8.3.2 The letter will state the expectations of the FRC, as well as any further actions being considered by the Centre such as administrative or civil actions.

8.3.3 You should develop and implement an action plan to rectify all deficiencies in a timely manner. Note that the FRC may decide to conduct a follow-up examination at a later date to confirm that you have addressed the deficiencies and have implemented your action plan in a timely manner. It is important that you follow your action plan and that you maintain proper records of what was done to address the deficiencies.

8.3.4 The Centre will send additional correspondence notifying your organization of their final decision.

8.3.5 Remember to always document your progress. Documentation is important when demonstrating that you are complying with the AML Legislation and that you have addressed those deficiencies as stated in your action plan letter to the FRC.

9 Appendix

9.1. Guidance to implementing the Risk Based Approach

1	Accountants should take appropriate steps to identify and assess the risk firm-wide, given their particular client base, that they could be used for ML/TF. Although individual accountants are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of business relationships.
2	Money Laundering and Terrorism Financing risks are grouped in three main categories; (i) Country/Geographic Risk (ii) Client Risk (iii) Transaction/Service/Channel Risk
3	Accountants, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.
4	Although there is no universally accepted set of risk categories, the examples provided in this checklist are the most commonly identified risk categories.
5	An accountant may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority.
	The risks and red flags listed in each category are not exhaustive but provide a starting point when designing the RBA
Country/Geographic Risk	
1	A client may be at a higher risk when features of their business are connected to a higher risk country as regards;
(a)	Origin, or current location of the source of wealth or funds;
(b)	Where the services are provided;
(c)	Client's country of incorporation or domicile;
(d)	Location of the client's major operations;
(e)	Beneficial owner's country of domicile; or
(f)	Target company's country of incorporation and location of major operations (for potential acquisitions).

2	Higher risk countries may be considered as those that are specifically identified by credible sources to;
(a)	Have significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling;
(b)	Be subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations;
(c)	Have weak governance, law enforcement, and regulatory regimes, including countries identified as having weak AML/CFT regimes; or
(d)	Be uncooperative in providing beneficial ownership information to competent authorities.
	Client risk
3	The firm's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.
4	The firm's clients include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients
5	Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as;
(a)	Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares,
(b)	Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.
(c)	Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities or other factors are not consistent with the accountants' understanding of the client's business and economic purpose.
6	Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
7	Clients that are cash (and/or cash equivalent) intensive businesses. Where such clients are themselves subject to and regulated for a full range of AML/CFT requirements. These may include;
(a)	Money or Value Transfer Services (MVTS) businesses (e.g. remittance houses, currency exchange houses, casas de cambio, centros cambiarios, remisores de fondos, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities);
(b)	Operators, brokers and others providing services in virtual assets
(c)	Casinos, betting houses and other gambling related institutions and activities;
(d)	Dealers in precious metals and stones
8	Businesses that while not normally cash intensive appear to have substantial amounts of cash.
9	Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
10	Clients using financial intermediaries, financial institutions or non-financial institutions are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities
11	Clients who appear to be acting on somebody else's instructions without disclosure
12	Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons
13	Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible to perform a proper risk assessment.
14	Clients with previous convictions for crimes that generated proceeds, who instruct Accountants (who in turn have knowledge of such convictions) to undertake specified activities on their behalf

15	Clients who have no address, or multiple addresses without legitimate reasons.
16	Clients who have funds that are obviously and inexplicably disproportionate to their circumstances such as their age, income, occupation or wealth.
17	Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.
18	Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.
19	Clients who offer to pay unusually high levels of fees for services that would not ordinarily warrant such a premium
20	Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.
21	Where there are certain transactions, structures, geographical location, international activities or other factors that are not consistent with the accountants' understanding of the client's business or economic situation
22	Clients who are suspected to be engaged in falsifying activities through the use of false loans, false invoices, and misleading naming conventions
23	The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership
24	The relationship between employee numbers/structure and nature of the business is divergent from the industry norm such as the turnover of a company is unreasonably high considering the number of employees and assets used compared to similar businesses.
25	Sudden activity from a previously dormant client without any clear explanation.
26	Clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enter into new/emerging markets. Organized criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.
27	Indicators that the client does not wish to obtain necessary governmental approvals/filings, etc.
28	Reason for client choosing the accountant is unclear, given the firm's size, location or specialization
29	Frequent or unexplained change of client's professional adviser(s) or members of management
30	Clients are reluctant to provide all the relevant information, or one has reasonable grounds to suspect that the information provided is incorrect or insufficient.
31	Clients seeking to obtain residents rights or citizenship in the country of establishment of the Accountants in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.
	Transaction/Service and associated delivery channel risk
	Services which may be provided by Accountants and which (in some circumstances) risk being used to assist money launderers may include;
32	Use of pooled client accounts or safe custody of client money or assets without justification.
33	Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary for instance, naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage. It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.
34	In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting as trustees of such a trust.
35	Services which may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.

36	Services that are capable of concealing beneficial ownership from competent authorities.
37	Services requested by the client for which the accountant does not have expertise except where the accountant is referring the request to an appropriately trained professional for advice.
38	Non-cash wire transfers through the use of many inter-company transfers within the group to disguise the audit trail.
39	Services that rely heavily on new technologies such as in relation to initial coin offerings or virtual assets that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.
40	Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
41	Transactions where it is readily apparent to the accountant that there is inadequate consideration, where the client does not provide legitimate reasons for the transaction.
42	Administrative arrangements concerning estates where the deceased was known to the accountant as being a person who had been convicted of proceeds generating crimes.
43	Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances and in the experience of the accountant.
44	Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason
45	Transactions using unusual means of payment such as precious metals or stones.
46	The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.
47	Unexplained establishment of unusual conditions/clauses in credit arrangements that do not reflect the commercial position between the parties and may require Accountants to be aware of risks. Arrangements that may be abused in this way might include unusually short/long amortization periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or other security instruments substantially ahead of the maturity date initially agreed.
48	Transfers of goods that are inherently difficult to value for instance jewels, precious stones, objects of art or antiques, virtual assets, where this is not common for the type of clients, transaction, or with accountant's normal course of business such as a transfer to a corporate entity, or generally without any appropriate explanation.
49	Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.
50	Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason
51	Power of representation given in unusual conditions for instance when it is granted irrevocably or in relation to specific assets and the stated reasons for these conditions are unclear or illogical.

52	Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reasons.
53	Situations where a nominee is being used such as a friend or family member is named as owner of property/ assets where it is clear that the friend or family member is receiving instructions from the beneficial owner with no apparent legal, tax, business, economic or other legitimate reason.
54	Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
55	Commercial, private, or real property transactions or services to be carried out by the client with no apparent legitimate business, economic, tax, family governance, or legal reasons.
56	Existence of suspicions regarding fraudulent transactions, or transactions that are improperly accounted for. These might include
(a)	Over or under invoicing of goods/services
(b)	Multiple invoicing of the same goods/services
(c)	Falsely described goods/services – over or under shipments such as false entries on bills of lading.
(d)	Multiple trading of goods/services.
	In relation to the areas of risk identified above, Accountants may also consider the examples of fraud risk factors listed in International Standard of Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240) and the examples of conditions and events that may indicate risks of material misstatement in International Standard of Auditing 315: Identifying and assessing risks of material misstatement through understanding the entity and its environment (ISA315). Even where the accountant is not performing an audit, ISA 240 and ISA 315 provide helpful lists of additional red flags.
	General factors that may increase risk
1	Unexplained urgency of assistance required
2	Unusual sophistication of client, including complexity of control environment
3	Unusual sophistication of transaction/scheme
4	The irregularity or duration of the client relationship. One-off engagements involving limited client contact throughout the relationship may present higher risk.
	Factors that may decrease risk
1	Involvement of adequately regulated financial institutions or other Designated Non-Financial Businesses and Professions (DNFBPs).
2	Similar country location of the Accountant and client.
3	Role or oversight of a regulator or multiple regulators.
4	The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact and easy flow of information throughout the relationship may present less risk.
5	Private companies that are transparent and well-known in the public domain.
6	Accountant's familiarity with a particular country, including knowledge of and compliance with local laws and regulations as well as the structure and extent of regulatory oversight.
	FIRM-WIDE RISK ASSESSMENT
1	The firm should perform a firm-wide risk assessment that takes into account the size and nature of the practice; the existence of high-risk clients (if any); and the provision of high-risk services (if any). Once completed, the firm-wide risk assessment will assist the firm in designing its policies and procedures

2	Depending on the size of the firm, the types of services provided, the risk profile of clients and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole practitioners, providing limited services to low risk clients, client acceptance may be reserved to the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms, serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary
3	Develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients.
4	Design engagement acceptance policies. Specifically, one should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime.
5	Exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. These cases would trigger reporting obligations with the Financial Reporting Centre.
6	Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the RBA. Senior management must create a culture of compliance, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.
7	The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:
(a)	Designating an individual or individuals, at management level responsible for managing AML/CFT compliance;
(b)	Designing policies and procedures that focus resources on the firm's higher-risk, services, products, clients and geographic locations in which their clients/they operate, and include risk-based CDD policies, procedures and processes;
(c)	Ensuring that adequate controls are in place before new services are offered; and
(d)	Ensuring adequate controls for accepting higher risk clients or providing higher risk services, such as management approval.
8	Consider using proven technology-driven solutions to minimize the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the needs of Accountants as they continue to develop, this may be particularly important for smaller firms that may be less able to commit significant resources of time to these activities.
9	The most effective tool to monitor the internal controls is a regular (typically at least annually) independent (internal or external) compliance review. If carried out internally, a staff member that has a good working knowledge of the firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the firm's procedures.
10	The firm-wide risk assessments should be reviewed / updated regularly and ensure that policies and procedures continue to target those areas where the ML/TF risks are highest.
	Documenting the Risk Assessment
1	It is critical for the accountant to document the risk assessments in order to be able to demonstrate their basis and exercise due professional care and use compelling good judgement
2	Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment and dated. In assessing the risk profile of the client at this stage, reference must be made to the relevant targeted financial sanctions lists to confirm neither the client nor the beneficial owner is designated and included in any of them.

3	A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship.
4	The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties.
	Mitigating Risks Assessed
1	Implement policies, controls and procedures that effectively manage and mitigate identified risks.
2	They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and supervisors. Measures and controls may include:
(a)	General training on ML/TF methods and risks relevant to accountants
(b)	Targeted training for increased awareness to Accountants providing specified activities to higher risk clients or undertaking higher risk work.
(c)	Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence and record source of wealth and beneficial ownership information if required.
(d)	Periodic review of the services offered by the accountant, and the periodic evaluation of the AML/CFT framework applicable to the accountant and the accountant's own AML/CFT procedures, to determine whether the ML/TF risk has increased.
(e)	Reviewing client relationships from time to time to determine whether the ML/TF risk has increased.

Institute of Certified Public Accountants of Kenya
CPA Centre, Thika Road
P. O. Box 59963 - 00200 Nairobi Kenya
Telephone: +254 (020) 2304226, 2304227
Fax: +254 (020) 8562206
Mobile: +254 727 531006 / 733 856262 /
721 469796 / 721 469169
Email: icpak@icpak.com
www.icpak.com

Supported and funded by

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH