REPUBLIC OF KENYA
FINANCIAL REPORTING CENTRE
OLD MUTUAL TOWER, UPPER HILL, UPPER HILL ROAD
PRIVATE BAG 00200, NAIROBI TEL: +254 709858000

DUE DILIGENCE GUIDANCE FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

MARCH 2025

Contents

Abbreviations:

AML	Anti-Money Laundering
CDD	Customer due diligence
CFT	Combatting of Terrorism Financing
DNFBPs	Designated Non-Financial Businesses and Professions
ML	Money Laundering
PF	Proliferation Financing
POCAMLA	Proceeds of Crime and Anti-Money Laundering Act
TF	Terrorism Financing

1.0 Introduction

1.1 This Due Diligence Guidance has been prepared in accordance with the requirements of the Proceeds of Crime and Anti-Money Laundering Act, 2009 (Herein referred to as POCAMLA) and the Proceeds of Crime and Anti-Money Laundering Regulations, 2023 (herein referred to as POCAML-Regulations).

1.2 To ensure effective implementation and compliance with the Anti-Money Laundering (AML) and Combatting of Terrorism Financing (CTF) requirements, POCAMLA gives the Financial Reporting Centre (*herein referred to as FRC*) the powers under Section 36A to regulate and supervise reporting institutions and Section 24A to issue instructions and directions, either specific or general.

1.3 Due diligence requirements are provided in POCAMLA, section 45-46 and Part IV of POCAML-Regulations. They broadly include requirements relating to:

a) Customer due diligence
b) Enhanced due diligence
c) Politically exposed persons
d) Beneficial ownership
e) Ongoing due diligence

1.4 The due diligence requirements should be implemented by all Designated Non-Financial Businesses and Professions (DNFBPs) in Kenya defined under Section 2 of POCAMLA. They include accountants, advocates, dealers in precious stones and dealers in precious metals, real estate agencies, casinos, and trusts and company service providers.

1.5 This Guidance is intended to guide DNFBPs on the appropriate practices while conducting due diligence.

1.6 The CDD Guideline is not intended to replace the existing AML/CFT laws and regulations but rather to provide supervisory and prudential clarity on the context of compliance within the framework of the AML/CFT laws, regulations as well as international standards for AML/CFT regarding due diligence.

2.0 Purpose of the customer due diligence Guidance

2.1 The purpose of this document is to provide practical guidance to entities regarding customer due diligence. It is provided to assist DNFBPs with day-to-day compliance.

2.2 This Guidance is aimed at ensuring that the DNFBPs:

(a) identify and verify the identity of a customer using reliable, independent source documents, data or information.

(b) identify and verify the identity of a person acting on behalf of a customer and the authority to act on behalf of the person or customer.

(c) identify beneficial owners, and take reasonable measures to verify the identity of beneficial owners and ascertain the ownership and control structure in the case of legal persons and arrangements

(d) obtain information relating to the purpose and nature of the business relationship, and

(e) ensure that any transaction being conducted is consistent with the DNFBPs' knowledge of the customer or business relationship, their nature of business and risk profile, including where necessary, the source of wealth or funds.

3.0 What is Customer Due Diligence?

3.1 Customer due diligence (CDD) is the process of collecting a series of identification information on an applicant or customer and verifying its validity and legitimacy in order to establish and/or maintain a business relationship. The purpose of CDD is for you to know who you are conducting business with to mitigate money laundering (ML), terrorism financing (TF) and proliferation financing (PF) risks.

3.2 Section 2 of POCAML-Regulations defines:

"*applicant*" as a person or legal arrangement seeking to form a business relationship, or to carry out a one-off transaction, with a reporting institution;

"*customer*" in relation to a transaction or an account, include;

a) the person or legal arrangement in whose name a transaction or account is arranged, opened or undertaken;
b) a signatory to a transaction or account;
c) any person or legal arrangement to whom a transaction has been assigned or transferred;
d) any person or legal arrangement who is authorized to conduct a transaction; or
e) such other person or legal arrangement as the Centre may specify.

4.0 Importance of Customer Due Diligence

To confirm the identity of customers: Be certain who the DNFBP is dealing with and ensure that the DNFBP is not dealing with listed entities/ persons under the TFS regime (see 'screening' for more information on this).

To enable risk profiling of customers: CDD ensures the DNFBP has the required information to profile customers and assess the money laundering/terrorism financing (ML/TF) risk the customer may pose to your business or organization.

To prevent abuse by criminals: Criminals sometimes use proxies or appoint another person to conduct transactions on their behalf. This helps shield their own identity. Without proper CDD, the RI may unwittingly be helping a criminal launder money or financing terrorism

To comply with AML/CFT laws and regulations: Implementation of CDD measures is one of the AML/CFT obligations for all DNFBPs.

To safeguard reputation: CDD helps to protect the DNFBPs' reputation and the integrity of entire financial systems by reducing the likelihood of a DNFBP becoming a vehicle for or a victim of financial crime and suffering the consequential reputational damage.

5.0 When to carry out CDD

5.1 DNFBPs should carry out CDD when:

a) establishing initial business relations;
b) undertaking occasional or one-off transactions;
c) there is cause to be suspicious of money laundering and terrorism financing; and
d) there is doubt about the veracity or adequacy of previously obtained customer information including identification data.

5.2 The customer due diligence processes entail:

(a) identification of an applicant or customer of who may be:
  i. natural persons
  ii. legal persons
  iii. partnerships
  iv. trusts

(b) verifying the identity of the applicant or customer using reliable, independent source documents, data or information.

(c) identifying and taking reasonable measures to verify the identity of a beneficial owner.

(d) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(e) if another person is acting on behalf of the customer, identifying and verifying the identity of that other person, and verifying that person's authority to act on behalf of the customer.

6.0 Customer identification and verification

6.1 DNFBPs should obtain reliable documents for the identification and verification of customers. This must be performed under all circumstances which require DNFBPs to undertake CDD measures.

Table 1: CDD Information and Documentation

	CDD Information	**CDD Documentation**
Natural Persons	✓ Full name of the person ✓ Postal address; ✓ Current physical or residential address; ✓ Mobile telephone number; ✓ Occupation or employment details; ✓ Source of income; ✓ Nature and location of business activity; ✓ Kenya Revenue Authority Personal Identification Number (KRA PIN); ✓ where applicable, written references from acknowledged persons attesting to the customer's identity.	✓ Birth certificate (In case of minors) ✓ National identity card ✓ Driver's license ✓ Valid Passport (Mandatory for foreign nationals) ✓ KRA PIN Certificate
Legal Persons	❖ Registered name; ❖ Address of the registered office and, if different, a principal place of business; ❖ The full name, date of birth, identity or passport number and address of the natural persons managing, controlling or owning the body	❖ Certificate of registration or certificate incorporation; ❖ CR12 ❖ BOF1 ❖ A corporate resolution authorizing a person to act on behalf of the body corporate together with a copy of the latest annual return submitted in respect of the body corporate in accordance with the law under which it is established;

	corporate or legal entity; ❖ KRA PIN	❖ KRA PIN Certificate ❖ The Act establishing the body corporate where applicable; ❖ For corporate bodies, audited financial statements for the last full year; ❖ for sole traders, un-audited financial statements for the last full year:
Partnership	• Name of the partnership or where applicable its registered name; • Registered address or principal place of business or office; • Registration number; • The full name, date of birth, identity card number or passport number and address of every partner; • The person who exercises executive control over the partnership; • The name and particulars of each natural person who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting institution on behalf of the partnership.	• Certificate of Registration • The Partnership Deed • KRA PIN of the partnership or the Partners • Un-audited financial statements for the last full year
Trust	➢ Registered name; ➢ Registration number;	➢ Evidence of registration or incorporation such as a Certificate of Incorporation or registration;

	➢ Registered office and if different the principal place of business; ➢ Full names of the trustee, beneficiaries or any other natural person exercising ultimate effective control over the trust; ➢ Full name of the founder of the trust; NB: *In cases where a settlor, trustee, protector, beneficiary, etc., is not an individual apply CDD measures for a legal person or arrangements.*	➢ Trust deed; ➢ Formative document ➢ Any other documentation from a reliable independent source proving the name, form and current existence of the customer; and

6.1 DNFBPs should verify the identity of the customer/applicant using reliable, independent source documents, data or information. Independent sources for verification of customer identity include government databases (Government IPRS system, KRA Pin Checker, BRS), open sources, as well as physical examination of government issued identification documents (refer to section 6.1 above).

6.3 DNFBPs should understand and obtain appropriate information on the purpose and intended nature of the business relationship. Depending on the type of customer, the information may include but is not limited to the following examples:

(i) information concerning the customer's or beneficial owner's business or occupation/employment.

(ii) information on the types of products or services or distribution channels which the customer intends to use.

(iii) the anticipated level and nature of the activity that is to be undertaken through the business relationship, which may include the number, size and frequency of transactions.

(iv) any relevant information about related third parties and their relationships with the customer.

6.5 The DNFBP's understanding of the customer's profile begins with obtaining the relevant information on the purpose and nature of the business relationship, and this is expected to improve over time as the DNFBP learns more about the customer, their use of products and the services that they require.

7.0 Timing of verification

DNFBPs should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

(a) this occurs as soon as reasonably practicable
(b) this is essential not to interrupt the normal conduct of business and
(c) the ML/TF risks are effectively managed.

8.0 Identification and verification of beneficial owners

DNFBPs should identify the beneficial owners of customers who are legal persons or legal arrangements and take reasonable measures to verify their identity, that is:

a) For a legal person, identify and verify the natural person(s) who ultimately has a controlling ownership interest.
b) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust including through a chain of control or ownership.
c) Where there is no natural person is identified, DNFBPs should identity the relevant natural person(s) who holds the position of senior managing official.

9.0 Customer Risk Rating

9.1 DNFBPs should understand the ML/TF risks of their customers, referred to as the customer risk profile or risk rating. The process of determining customer risk profiles should be sufficiently detailed to distinguish between the different risk ratings of the customers.

9.2 The assessment of the customer risk profile is specific to each DNFBP and a conclusion regarding the customer risk profile should be based on consideration of all pertinent customer information. There are no required risk profile categories (for example it is common to use the three (03) scale approach of; Low, Medium and High) and the number and detail of these categorizations will vary based on the DNFBP size and complexity.

9.3 The DNFBP should identify the specific risks of the customer and then analyze all pertinent information to develop the customer's risk profile. In determining a customer's risk profile, the DNFBP should consider risk factors, such as:

(i) Type of customer
(ii) Type of customer's business
(iii) Products and services
(iv) Delivery channels
(v) Geographic locations

9.4 The above risk factors should be reviewed on an ongoing basis and the existence of any one single indicator is not necessarily determinative of the existence of a lower or higher customer risk profile.

9.5 As with the risk assessment, the DNFBP may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer's business, delivery channels, or the geographic location where the customer does business, may pose a higher risk of ML/TF.

9.6 The risk profile of a customer will determine the extent of CDD measures to be undertaken as follows:

a) where the higher ML/TF risk has been identified, the DNFBP should conduct enhanced due diligence measures on the customer.
b) Where the medium ML/TF risk has been identified, standard CDD measures should apply.
c) where the lower ML/TF risk has been identified, the DNFBP should apply simplified due diligence (SDD) measures but this does not apply to cases involving suspicion of ML/TF.

9.7 In order to determine the risk profile of a customer, DNFBPs should take into account a range of factors. Some of the main factors to consider for high and low risk are explained in the boxes below.

High-risk factors

There are circumstances where the risk of ML/TF is high, and enhanced CDD measures have to be taken. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher risk situations may include the following:

(i) ***Customer risk factors:*** *Examples include, the business relationship being conducted in unusual circumstances (e.g. significant unexplained geographic distance between the DNFBP and the customer), non-resident customers, legal persons or arrangements that are personal asset-holding vehicles, companies that have nominee shareholders or shares in bearer form, business that are cash-intensive, the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.*

(ii) ***Country or geographic risk factors****: Examples include countries identified by credible sources, such as Financial Intelligence Authority, Mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems, countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations, countries identified by credible sources as having significant levels of corruption or other criminal activity, countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.*

(iii) *Product, service, transaction or delivery channel risk factors: Examples include, private banking, anonymous transactions (which may include cash), non-face-to-face business relationships or transactions, and payment received from unknown or un-associated third parties.*

Low Risk Factors

There are circumstances where the risk of ML/TF may be low. In such circumstances and provided there has been an adequate analysis of the risk by the DNFBP consistent with the ML/TF National Risk Assessment, the DNFBP may apply simplified CDD measures. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower-risk situations include the following:

(i) ***Customer risk factors:*** *Examples include, other DNFBPs where adequate AML/CFT oversight is being undertaken, public companies listed on a stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, public administrations or enterprises, salary earners, SME entities.*

(ii) ***Product, service, transaction or delivery channel risk factors****: Examples include residents using interbank transfers, ATMs, children accounts, elderly accounts, financial products or services that provide* *appropriately defined and limited services to certain types of customers, to increase access for financial inclusion purposes.*

(iii) ***Country risk factors:*** *Examples include countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems and countries identified by credible sources as having a low level of corruption or other criminal activity.*

10.0 Types of Customer due diligence measures

10.1 Simplified Due Diligence

Simplified due diligence is the lowest level of due diligence that can be conducted on a customer. Simplified customer due diligence measures may be applied under the following circumstances:

a) Where lower risks have been identified, through an adequate analysis of risks by the country or the reporting institution; and
b) Where the simplified measures are commensurate with the lower risk factors.

DNFBPs should obtain sufficient information on the risk factors to enable them to be reasonably satisfied that their assessment of the ML/TF risk associated with the customer is low and justified.

Additionally, DNFBPs should be aware that the ML/TF risks could change from the time of onboarding a customer. Upon change of the risk levels, DNFBPs should apply either standard or enhanced due diligence measures as appropriate.

DNFBPs should note that simplified customer due diligence measures shall not be applied whenever there is suspicion of money laundering, terrorism financing or proliferation financing, or where specific higher risk scenarios apply.

Implementing simplified due diligence measures does not exempt any DNFBP from reporting any suspicious transactions to FRC.

Examples of Simplified CDD measures:

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship

- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

11.2 Standard Due Diligence (SDD)

Standard due diligence is applicable in situations where there is a potential ML/TF risk but it is unlikely that these risks will be realized. Standard due diligence should be applied to all clients, unless simplified due diligence or enhanced due diligence is appropriate.

Examples of Standard CDD measures:

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information.
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the DNFBP is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required.
- Understanding and obtaining information on the purpose and intended nature of the business relationship.
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the business and risk profile of the client, including where necessary the sources of wealth and funds.

11.3 Enhanced customer due diligence (EDD)

Enhanced due diligence (EDD) measures shall be applied to persons and entities that present a higher risk to the DNFBP. In addition to the standard customer due diligence measures, the EDD measures that should be applied are as follows:

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

EDD must be applied in the following scenarios;

i. Foreign Politically exposed persons (PEPs) and domestic PEPs assessed as high-risk
ii. High-risk countries, customers and transactions as identified by the DNFBP
iii. Where higher risks are identified at national, sectoral or entity levels

iv. Business relationships and transactions with any natural and legal persons or legal arrangements originating from countries identified as posing a higher risk of money laundering, terrorism financing or proliferation by the;

  a) Financial Action Task Force (FATF) (as having strategic money laundering and combating financing of terrorism deficiencies, that have not made sufficient progress in addressing the said deficiencies or have not committed to an action plan to address the deficiencies);

Examples of Enhanced CDD Measures:

- Obtaining additional information on the customer or beneficial owner (e.g. occupation, source of wealth/fund, information available through public databases, internet), and updating more regularly the identification data of such persons and sources which can be regarded as credible.
- Obtaining information on the reasons for intended or performed transactions carried out by the customer.
- Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the customer and evidencing this through appropriate documentation obtained.

  Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile.

  Considering the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime. This could include obtaining appropriate documentation concerning the source of wealth or funds
- Increasing the frequency and intensity of transaction monitoring
  - ✓ Obtaining the approval of senior management to commence or continue the business relationship.
  - ✓ Conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting the patterns transactions that need further examination.

11.0 Ongoing Due Diligence

13.1 DNFBPs should conduct ongoing due diligence on a continuous basis depending on the risk associated with the customer by:

  a. scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the customer, their business and risk profile, including where necessary, the source of funds. Where the activities of the client are not consistent with the DNFBP's knowledge of the client or the purpose of the intended nature of business relationship, the DNFBP should assess if there's suspicion of ML/TF. Confirmed suspicion of ML/TF should be reported to the FRC.

b. ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

13.2 The frequency of undertaking ongoing CDD on existing customers will be determined by the risk rating assigned to a particular customer. Customers whose ML/TF risk was assessed as "High" should be reviewed more frequently than customers whose risk is "Low". In addition, some circumstances where review of customer due diligence may be triggered include, but not limited to:

(a) Significant and unexplained changes in account activity
(b) Changes in employment or business operation
(c) Changes in ownership of a business entity
(d) Red flags identified through suspicious activity monitoring
(e) Results of negative media search programs
(f) Length of time since customer information was gathered and the customer risk profile assessed.
(g) Changes in legislation and regulatory requirement.

12.0 Sanction screening process.

DNFBPs should screen customers against United Nation Security Council Resolutions (UNSCR) and domestic sanctions lists at onboarding for new customers and existing customers. Sanction screening must also be conducted on an ongoing basis for the existing customers following updates to the sanctions lists.

13.0 Record keeping

DNFBPs should develop clear policies and procedures for record keeping of customer identification and transactions records and the retention period.

All information, records and documents obtained through CDD measures need to be kept for a minimum period of seven years from the date the relevant business or transaction was completed or following the termination of a business relationship.

This includes:

a. records obtained through customer due diligence measures such as copies or records of official documents like passports, national identification cards or similar documents,
b. Evidence of sanction screening,
c. account files,
d. business correspondence, and
e. the results of any analysis undertaken such as inquiries to establish the background and purpose of complex, unusual, large transactions.

These records should be made available on a timely basis to domestic competent authorities as and when required.

14.0 Politically Exposed persons

16.1 Politically exposed person (PEP) refers to a person who has been entrusted with a prominent public function in Kenya or another jurisdiction. They include:

a) members of Cabinet;
b) senior executives of state owned corporations;
c) important political party officials;
d) senior military officials and other senior members of the disciplined forces;
e) members of the Judiciary;
f) State Officers;
g) senior Public Officers;
h) senior Officials of International Organization;
i) Heads of State or Government; and
j) immediate family member or close associate of persons listed above.

16.2 The family members of a PEP are individuals who are related to a PEP either by blood or through marriage or similar (civil) forms of partnership while close associates are individuals who are closely connected to a PEP, either socially or professionally.

16.3 DNFBPs should consider a range of factors when determining whether a particular holder of a prominent public function has the requisite seniority, prominence or importance to be categorized as a PEP. The relevant factors could include:

(a) Assessing the individual's vulnerability to corruption as per various publicly available independent sources.
(b) The official responsibilities of the individual.
(c) Nature of the title (honorary or salaried prominent public function),
(d) The level of authority of the individual over governmental activities and other officials,
(e) Whether the function affords the individual access to significant government assets and funds or the ability to direct the awards of government tenders or contracts and
(f) Whether the individual has links to an industry particularly prone to ML/TF abuse.

DNFBPs should take reasonable measures to determine whether customers or beneficial owners are PEPs. PEPs are categorised into three; domestic, foreign and international organisation PEPs. Foreign PEPs are always considered high risk and require the application of enhanced due diligence measures as discussed in section 11.3 above.

Where a customer or beneficial owner is a domestic or international PEP, DNFBPs should undertake ML/TF risk assessment of the PEP's business relationship to determine the risk profile of the PEP and take commensurate level of CDD.

Sources of information that can be used to assist DNFBPs in determining if a customer or beneficial owner is a PEP include:

- Customer self-declarations
- Internet and media searches
- Public database e.g. gazette notices by the Independent Electoral and Boundaries Commission of Kenya of Elected members during the national elections and of Political Party Officials in Kenya, list of information on Heads of Government Ministries, Departments and Agencies, Judicial Service Commissions, Ministry of Defense and other publicly available credible information
- Commercial database
- In-house databases and information sharing within associations members

DNFBPs should regularly review their existing customers to identify PEPs who may already exist in their database or business relationships and immediately update the identified PEP onboarding documents by performing the procedures required for PEPs.

15.0 Non-face-to-face customers

DNFBPs may encounter situations where the customer does not present himself/herself (non-face-to-face) when establishing business relationship and conducting transactions. Such business relationships and transactions present higher risks. The CDD measures identified above for face-to-face customers apply to non-face-to-face customers. Additionally, DNFBPs must identify the higher risks associated with non-face-to-face business relationships or transactions and apply commensurate due diligence measures as appropriate.

The measures taken by a DNFBP to verify the identity in these circumstances will depend on the nature and characteristics of the product or service provided and the client/customer's risk profile.

DNFBPs should institute specific and adequate measures to mitigate the higher risk, for example:

(a) Certification of documents presented
(b) Requisition of additional documents
(c) Telephone contact with the customer at a residential or business number that can be verified independently
(d) Confirmation of the customer's address through an exchange of correspondence or other appropriate method

(e) Telephone confirmation of the customer's employment status with his/her employer's human resource department at a listed business number of the employer
(f) Confirmation of the customer's salary details by requiring the presentation of a recent job letter or bank statement, where applicable; or
(g) Video calls with the customer.

16.0 Eligible or Group Introducers

An eligible introducer means any person who introduces an applicant for business to a reporting institution in Kenya, and

a) is regulated under the Act or any similar legislation in an equivalent jurisdiction, or is subject to rules of professional conduct relating to the prevention of money laundering; and
b) is based either in Kenya or in an equivalent jurisdiction

A group introducer means an introducer who is part of the same group as the reporting institution to whom the applicant for business is introduced and is, for anti-money laundering purposes is subject to the anti-money laundering regulations of a regulator in Kenya or in an equivalent jurisdiction.

Where a customer is introduced to a DNFBP by an eligible introducer or a group introducer, DNFBPs should:

a) Obtain and maintain documentary evidence that the eligible introducer or group introducer is regulated for the purposes of preventing money laundering, terrorism financing and proliferation financing; and
b) Satisfy themselves that the procedures laid down by the eligible introducer or group introducer meet the requirements specified in the AML/CFT/CPF Laws, or any code or guidelines issued by a supervisory body.
c) Satisfy themselves that they may obtain customer identification documentation from the group introducer upon request.

17.0 Reliance on third parties

DNFBPs may rely on third parties to perform elements of the customer due diligence measures or to introduce business, provided that:

a) The third party is a financial institution or DNFBP or a person that is supervised or monitored by a competent authority.
b) The DNFBP and third party have an agreement outlining the responsibilities of each party.
c) Copies of identification data and other relevant documentation relating to the CDD requirements are made available to the DNFBP without delay upon request

d) The third party is regulated, supervised or monitored by a competent authority and has measures in place for compliance with, CDD and record-keeping requirements in line with the POCAMLA and POCAML-Regulations.
e) Where a third party that is based in another country, the DNFBP shall assess the money laundering, terrorism financing and proliferation financing risks that the country poses and the adequacy of CDD measures adopted by reporting institutions in that country.

However, where the DNFBP relies on third parties, the ultimate responsibility for CDD measures remains with the DNFBP.

18.0 Failure to Complete CDD measures

Where an applicant for business does not supply evidence of identity as soon as reasonably practicable and the DNFBP is unable to complete the relevant CDD measure, the DNFBP should:

a) Not open the account
b) Not commence any business relationship with the customer
c) Not perform the transaction
d) File a suspicious transaction/activity report with the Centre

Where the DNFBP has commenced a business relationship with the customer it should:

a) Discontinue any transaction it is conducting for the customer.
b) End the business relationship or any understanding it has reached with the customer.

19.0 Tipping-off when Conducting CDD measures

Where a DNFBP forms a suspicion of money laundering or terrorism financing, and it reasonably believes that performing the customer due diligence process will tip-off the customer, the DNFBP is permitted not to pursue the customer due diligence process, and shall instead file a suspicious transaction/activity report to the Centre.

20.0 Training and awareness

Regulation 11 POCAML-Regulations stipulates that DNFBPs formulate, adopt and implement internal control policies, measures and other procedures proportionate to the size of the business to combat money laundering, terrorism financing and proliferation financing risks.

DNFBPs should develop and implement training programmes. The training programme should cover legal requirements and internal controls including CDD measures. The DNFBP should ensure that the staff and management are adequately trained to implement the DNFBP's CDD policies and procedures.

21.0 CDD policies and procedures

DNFBPs should establish and maintain written policies, procedures, processes, and controls in respect of CDD measures, which should form part of its overall AML compliance manual and communicate to all relevant employees

22.0 Review of the Guidance

This Guidance may be reviewed from time to time in line with updates in the AML/CFT/CPF laws, updates on the national, sectoral and institutional risk assessments, or any other circumstance that may necessitate a review, but in any case it shall be reviewed at least once every two years.