Central Bank of Kenya

Guidance on Customer Due Diligence (CDD)

August 2025

CONTENTS

ACRONYMS

AML	Anti-Money Laundering
BO	Beneficial Owner
BRS	Business Registration Service
CDD	Customer Due Diligence
CBK	Central Bank of Kenya
CBR	Correspondent Banking Relationship
CFT	Combating the Financing of Terrorism
CPF	Combating Proliferation Financing
DCP	Digital Credit Provider
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Taskforce
FI	Financial Institutions
FRC	Financial Reporting Centre
FXB	Foreign Exchange Bureau
KRA	Kenya Revenue Authority
IPRS	Integrated Population Registration Database System
MFB	Microfinance Bank
ML	Money Laundering
MMSP	Mobile Money Payment Service Provider
MRP	Money Remittance Provider
PEP	Politically Exposed Person
PF	Proliferation Financing
PF Regs.	The Prevention of Terrorism (Implementation of United Nations Security Council Resolutions on Prevention Suppression and Disruption of Proliferation Financing) Regulations
POCAMLA	The Proceeds of Crime and Anti-Money Laundering Act 2023
POTA	The Prevention of Terrorism Act
POCAML Regs.	The Proceeds of Crime and Anti-Money Laundering Regulations 2023
RBA	Risk-Based Approach
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
TF	Terrorism Financing
TF Regs.	The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression Terrorism Regulations.
TFS	Targeted Financial Sanctions
UN	United Nations
UNSCR	United Nations Security Council Resolution

PART I. PRELIMINARY

1.1 Title - Guidance on Customer Due Diligence (CDD)

1.2 Application

This Guidance applies to financial institutions (FIs) licensed under the Banking Act, the Microfinance Act, the Central Bank of Kenya (CBK) Act and the National Payment Systems Act:

i) Commercial banks;
ii) Mortgage finance companies;
iii) Microfinance banks;
iv) Money remittance providers;
v) Foreign exchange bureaus;
vi) Payment service providers; and
vii) Non-deposit taking credit providers (formerly known as digital credit providers).

1.3 Authorisation

This Guidance is issued pursuant to Section 36C(1)(d) of the Proceeds of Crime and Anti- Money Laundering Act (POCAMLA) which empowers the CBK to guide FIs on anti- money laundering, combating the financing of terrorism and proliferation financing (AML/CFT/CPF) issues.

1.4 Definitions[1]

1.4.1. "beneficial owner" means a natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted and includes any natural person who ultimately exercises effective control over a legal person or arrangement.

1.4.2. "customer" means in relation to a transaction or an account, specifically:
(a) a legal 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 authorised to conduct a transaction; or individuals or legal entities engaging in a business relationship with a FI. This could be a retail customer or a corporate client.

1.4.3. "competent authority" means a public authority other than a self-regulatory body with designated responsibilities for combating money laundering and terrorism financing.

1.4.4. "customer" in relation to a transaction or an account, includes—
(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 authorised to conduct a transaction.

[1] The Proceeds of Crime and Anti-Money Laundering Regulations 2023

1.4.5. "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.

1.4.6. "financial institution" means any person or entity, which conducts as a business, one or more of the following activities or operations—

(a) accepting deposits and other repayable funds from the public;

(b) lending, including consumer credit, mortgage credit, factoring, with or without recourse, and financing of commercial transactions;

(c) financial leasing;

(d) transferring of funds or value, by any means, including both formal and informal channels;

(e) issuing and managing means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money);

(f) financial guarantees and commitments;

(g) trading in —

(i) money market instruments, including cheques, bills, certificates of deposit and derivatives;

(ii) foreign exchange;

(iii) exchange, interest rate and index funds;

(iv) transferable securities; and

(v) commodity futures trading;

(h) participation in securities issues and the provision of financial services related to such issues;

(i) individual and collective portfolio management;

(j) safekeeping and administration of cash or liquid securities on behalf of other persons.

1.4.7. "legal persons" means any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, , partnerships, or associations and other relevantly similar entities.

1.4.8. "legal arrangements" means express trusts or any other similar entities.

1.4.9. "third party" means another financial institution or designated non-financial business or profession(DNFBP) or a person that is supervised or monitored by a competent authority.

PART II. STATEMENT OF POLICY

2.1 Purpose

The purpose of this Guidance is to:

i) Assist financial institutions (FIs) licensed by the CBK in complying with CDD requirements under the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA) and the regulations issued hereunder.

ii) Equip FIs with tools to manage related money laundering, terrorist financing and p proliferation financing (ML/TF/PF) risks.

iii) Uphold the integrity of the financial system by providing clarity on CDD processes, including customer identification, verification and ongoing monitoring.

2.2 Scope

This Guidance on (CDD) covers the identification, verification, and ongoing monitoring of customers, including risk-based assessments of individuals and entities. The Guidance outlines the procedures for managing risks related to money laundering, terrorist financing, and proliferation financing, in line with POCAMLA and its regulations.

2.3 Responsibility

The Board of Directors and Senior Management are responsible for ensuring the effective implementation of CDD measures by FIs. They must approve policies, allocate resources, and oversee staff training to meet regulatory requirements and manage risks. Additionally, they should regularly review and adapt CDD practices to ensure ongoing compliance and effectiveness.

2.4. Background

CDD plays a fundamental role in preventing financial crimes by ensuring that FIs can identify and assess the risks associated with their customers and their transactions. CDD lays the foundation for robust AML/CFT/CPF efforts, enabling FIs (FIs) to detect and prevent illicit activities while complying with regulatory requirements. By adopting robust CDD procedures, FIs not only ensure compliance with domestic laws and regulations but with international AML/CFT/CPF standards.

The CBK remains committed to preserving the integrity and stability of the country's financial system. In line with this commitment, it has developed this Guidance to assist the FIs it supervises with implementing CDD measures. This is through a risk-based approach, where FIs adopt CDD procedures tailored to the specific risks posed by each customer and transactions. This is in an effort to promote the consistent application of a risk- based approach to CDD across the sector. It aims to strike a balance between the goal of implementation of effective due diligence measures, while avoiding placing an undue burden on customers, fostering a more efficient and practical risk-focused compliance framework.

This Guidance draws from:

- The Financial Action Taskforce (FATF) Recommendations.
- The Mutual Evaluation of Kenya by the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) in 2021 and 2022.
- Results of the survey on Preventive Measures conducted by CBK in December 2024.

2.4.1. FATF Recommendation 10 on CDD

FATF Recommendation 10 highlights the importance of FIs implementing robust CDD procedures to effectively manage risks related to money laundering (ML), terrorist financing (TF), and proliferation financing (ML/TF/PF). The recommendation outlines several key measures, including identifying and verifying customers before establishing a business relationship or conducting transactions, as well as identifying and verifying beneficial owners, particularly for customers that are legal entities and arrangements.

FIs are also required to adopt a risk-based approach in their CDD procedures and continuously monitor transactions to identify suspicious activity and ensure consistency with the customer's profile. Enhanced Due Diligence (EDD) should apply in higher -risk situations, such as with politically exposed persons (PEPs) or transactions involving high- risk jurisdictions. Lastly, FIs must maintain records of CDD information and transactions to support potential investigations.

2.4.2. Key Findings of the Mutual Evaluation Report (MER) for Kenya 2022

An assessment of Kenya's AML/CFT/CPF legal and institutional framework was conducted between 2020 and 2021 by the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and the Mutual Evaluation Report published in September 2022.

Key findings regarding the implementation of CDD measures highlighted in the MER:

- Most FIs implement basic CDD and record-keeping practices, demonstrating a reasonable approach to identification and verification during customer onboarding and occasional transactions. Notably, banks and microfinance banks (MFBs), carry out these measures on an ongoing basis.
- Verification of information provided by foreign customers poses significant challenges for medium to large non-banking FIs (NBFIs), as they often lack access to independent, reliable verification sources.
- Regarding the verification of source of funds and wealth, the MER noted:
    - FIs fail to effectively verify source of funds or wealth through reliable, independent sources, often relying on customer declarations without validating the authenticity of supporting documents.
    - Many non-bank FIs (NBFIs) were unaware of the need to obtain source of wealth information, revealing gaps in their understanding of CDD requirements.

- Significant inadequacies were observed in identifying beneficial ownership (BO) and Politically Exposed Persons(PEPs) including:
    - Limited access to independent sources hampered their ability to verify the information gathered.
    - The systems for identifying politically exposed persons (PEPs) were notably ineffective, particularly for domestic PEPs.
    - International databases often failed to capture domestic PEPs, including their families and associates, leading FIs to rely on less robust methods and reducing the overall effectiveness of PEP identification and monitoring.

FIs are advised to refer to separate Guidance issued by CBK on Beneficial Ownership (BO) and PEPs.

2.4.3. CBK Survey on Preventive Measures

In December 2024, CBK conducted a survey on preventive measures: Key findings regarding CDD measures from the survey were as follows:

- Most FIs have CDD policies in place, reflecting progress made by FIs in complying with AML/CFT/CPF measures.
- The effectiveness of CDD policies depends heavily on the consistent implementation at institutional and operational levels.
- Outdated technological systems hinder the process of verifying customers.
- Most FIs struggled with the validation of foreign identity documents.
- There is a lack of standardized approaches to updating CDD across different financial sub-sectors.
- Regulatory requirements on CDD are perceived as complex, with inconsistencies in guidance and ambiguity around foreign entities.
- FIs face difficulties in communicating the importance of Know-Your-Customer (KYC) updates to customers.
- Persistent gaps in staff training and awareness limit the ability of FIs to adapt to evolving regulatory requirements and emerging financial crime risks.

PART III. OVERVIEW OF CUSTOMER DUE DILIGENCE MEASURES

3.1 Required Measures

Customer Due Diligence (CDD) is the process through which FIs collect, identify and verify information about customers with whom it intends to establish a business relationship or conduct a one-off or occasional transaction.

FIs are obliged to apply the following CDD measures to all customers as stipulated under Regulations 14 and 23 of the POCAML Regs:

(a) Identify the customer whether permanent or occasional and verify that customer's identity using reliable, independent source documents, data or information;

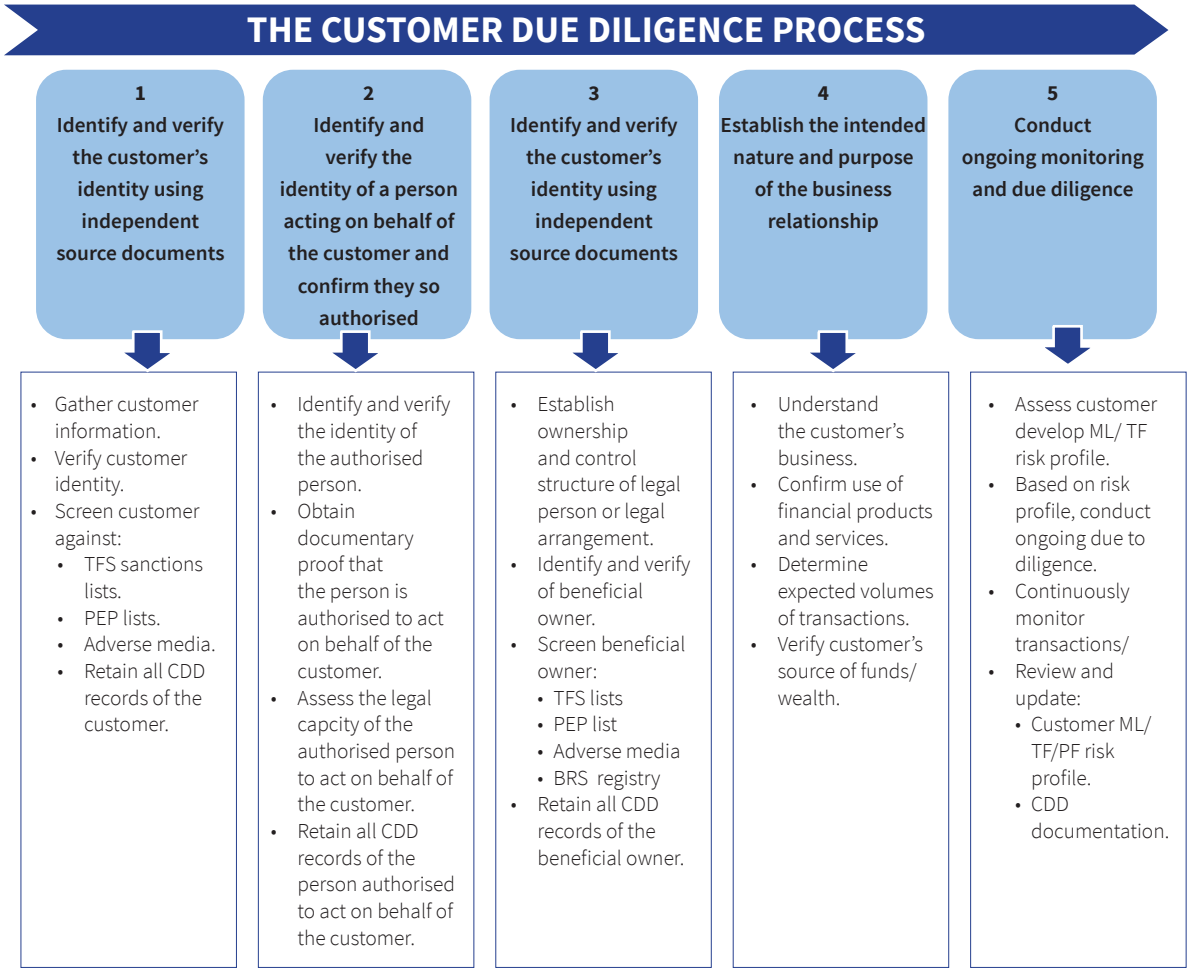
(b) Where a person purports to act on behalf of a customer, an FI should:
   i. verify that the person is so authorised to act; and
   ii. identify and verify the identity of the person authorized to act on behalf of the person.

(c) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that the reporting institution is satisfied that it knows who the beneficial owner is and it understands the ownership and control structure of the customer in case of legal persons and arrangements;

(d) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship;

(e) Conduct on going due diligence on the business relationship including:
   i. Scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the FIs knowledge of the customer, their business and risk profile, including where necessary, the source of funds.
   ii. 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.

Table 1: The Customer Due Diligence Process



3.2 When are FIs required to undertake CDD measures?

FIs are required to undertake CDD measures when:

(a) Establishing business relationships.

(b) Undertaking occasional or one-off transactions. This means the obligation to undertake CDD measures prior to opening an account or conducting a transaction applies to all transactions whether occasional or one-off transactions, regardless of the amounts in question. Kenya's AML/CFT/CPF legislation currently does not provide for thresholds or exemptions with regards to CDD. where FIs are permitted to open accounts without conducting CDD.

(c) When carrying out occasional transactions that are wire transfers under the circumstances covered by Regulation 32 of the POCAML Regs.

(d) When there is cause to be suspicious of money laundering, terrorist financing or proliferation financing, regardless of any exemptions or thresholds.

(e) When there is doubt about veracity or adequacy of previously obtained customer information including identification data.

3.3 Customer Identification and Verification

Prior to undertaking CDD, it is critical to distinguish between identifying the customer and verifying the customer's identity. Customer identification entails gathering of information on the prospective customer. Verifying the customer's identity involves confirming that the information provided to an FI is accurate and belongs to that individual or business. Verifying the customer helps ensure that the customer is an actual person and not using false or stolen identities. This done using reliable and independent sources like passports, national ID cards, company registries, or trusted electronic verification tools.

Specific CDD information requirements for natural persons, legal persons and legal persons are summarized in the **Table 2**. below:

Table 2: CDD information Requirements under POCMLA and POCAMLA Regs.

Legal Form	Type of Entity	POCAMLA	POCAMLA Regs.
Natural Person	Natural Person	S.45 (1)(1A)(a)	Reg. 15(1)
Legal Persons	• Private Limited Company • Public Limited Company • Foreign Company • Company Limited by Guarantee • Unlimited Companies	S.45(1)(1A)(b)	Reg.16(1)
	• Limited Liability Partnerships		Reg. 17(1)
Legal Arrangements	Trusts		Reg. 18(1)

3.3.1. CDD information requirements for natural persons

CDD information requirements specific to natural persons are highlighted under Section 45(1A)(a) of the POCAMLA and Regulation 15 (1) and (2) of the POCAML Regs. When identifying and verifying the identity of a natural person, FIs are required to obtain the following information:

i. Full name of the natural person;
ii. a birth certificate;
iii. a national identity card;
iv. a passport;
v. a driver's licence; and
vi. any other official means of identification as may be prescribed;

Additional documentation that can be used to verify the identity of a customer who is a natural person includes:

i. Postal address;
ii. Current physical or residential address;
iii. mobile telephone number;
iv. A recent utility bill, such as for electricity or water;
v. Occupation or employment details;
vi. Source of income;
vii. Nature and location of business activity;
viii. Income Tax Personal Identification Number (PIN) issued by the Kenya Revenue Authority, where available;
ix. Written references from recognised individuals attesting to the customer's identity, where applicable; and
x. For joint accounts, a written statement confirming that one party has personally known the other party or parties for at least twelve months.

3.3.2. CDD information requirements for legal persons

The FATF defines legal persons are defined as follows:

"Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities"

In Kenya, the legal persons registered with the Business Registration Service (BRS) include:

- Private Limited Companies;
- Public Limited Companies;
- Unlimited Companies;
- Companies Limited by Guarantee;
- Limited Liability Partnerships; and
- Foreign Companies;

Brief highlights on the different types of legal persons can be accessed under Annex I.

Regulation 16 (1) specifies to CDD information requirements for a legal person or which are:

i. The registered name of the entity;
ii. Documentary evidence of registration or incorporation, such as a certified copy of the Certificate of Registration or Certificate of Incorporation, the Memorandum and Articles of Association, or other equivalent documentation confirming the legal status of the entity.
iii. The address of the registered office and, if different, the principal place of business;
iv. A certified copy of a board resolution authorising the opening of an account or the conduct of business with the FI , and designating the individuals with signing authority;
v. The full name, date of birth, identity card or passport number, and residential address of the natural persons who manage, control, or own the legal entity;
vi. For corporate bodies, audited financial statements for the most recent full financial year;
vii. For sole proprietorships, unaudited financial statements for the most recent full financial year:
viii. The legal person's Personal Identification Number (PIN); and here applicable, a written confirmation from the customer's previous bank, confirming the customer's identity and account history.

3.3.3. CDD information requirements for legal arrangements (trusts)

Legal arrangements refers to express trusts and other similar legal arrangements.

Regulation 18 (1) stipulates the CDD information requirements for legal arrangements (trusts) are:

(a) its registered name;
(b) its registration number;
(c) evidence of registration or incorporation such as a Certificate of Incorporation or registration;
(d) trust deed;
(e) formative document such as partnership agreement, memorandum and articles of association;
(f) official returns showing registered office and if different the principal place of business;
(g) full name and details of the management company of the trust or legal arrangement, if any;
(h) names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement;

(i) full names of the trustee, beneficiaries or any other natural person exercising ultimate effective control over the trust;
(j) full name of the founder of the trust;
(k) any other documentation from a reliable independent source proving the name, form and current existence of the customer; and
(l) such other document or particulars as the FRC may specify.

3.3.4. Exemption from providing financial statements

Regulations 16 (g), 16 (h), and 17 (h) require FIs to obtain financial statements from customers that are corporate entities or sole proprietorships or partnerships. However, FIs should note that exemptions apply for customers who are newly registered entities that have been in existence for less than one year, or where practical difficulties prevent the timely submission of such statements. These provisions enable FIs to maintain flexibility while ensuring they have sufficient information that can be used to assess the customer.

3.4 Verifying the identity of the customer

Table 3: Examples of Customer Verification

(a) Verification of Details with Government Databases/Portals

- **National ID:** Cross-check to confirm that both the National ID number and serial number and name match the details contained in the Integrated Population Registration System (IPRS) database.
- **Passport:** Confirm with the IPRS that the National ID number located on the biodata page of the passport tallies with the identity details of the holder of the passport
- **Kenya Revenue Authority Personal Identification (PIN) Number KRA website.** Check that name indicated in the KRA PIN provided by the customer corresponds to that found on the website.

(b) Cross-check the customer's account opening details with details contained in the National ID or Passport:

- Full name (confirming that the full names appear in the exact same order and that the spelling is the same.
- Date of birth.
- Photograph: Confirm the physical likeness matches that of the customer applying to open an account or undertake a transaction or transactions.

(c) Biometric Authentication: Use facial recognition "selfie" to verify the customer's identity. This is particularly relevant for digital credit providers (DCPs) or mobile money service providers for the account opening process.

(d) Video Calls: Conduct video calls to verify the identity of the applicant and to confirm the physical presence of the applicant and match their image to the one provided in the identification document such as ID or passport.

3.4.1. Verifying the identity of Foreign Customers

When verifying the identity of foreign customers, FIs must adhere to the CDD requirements under the POCAMLA and POCAMLA Regs. The verification of foreign customers requires a careful approach to ensure compliance with the law while also addressing potential risks.

Steps FIs should follow to verify the identity of foreign customers:

Step 1: Obtain and Verify Official Identification Documents under the POCAMLA and POCAMLA Regs.

- **Passport:** The document for foreign customers is a valid passport that includes clear biometric details (e.g., photo, date of birth, nationality).

Step 2: Verify the Documents

- **Document authenticity:** Verify that the foreign documents are legitimate by checking the security features of the passport, visa, or other official identification documents. Use
- document verification tools, such as optical character recognition (OCR) software or third-party verification services, to detect fraud. The FIs can also obtain notarized passport copies.
- **Embassy Verification:** If there is any doubt about the authenticity of the documents, FIs can contact the customer's country's embassy in Kenya for verification.

Step 3: Consider additional CDD Measures such as:

- **Visa or Residence Permit:** For foreign individuals who are not citizens of Kenya but resident in Kenya, FIs may in addition to the passport, request a visa, work permit, or residence permit as proof of legal status and to verify their immigration status in Kenya.
- **Address Verification:**
  - **Utility Bills or Bank Statements:** For proof of the customer's address, request recent utility bills, rental agreements, or bank statements from their home country or from within Kenya.
  - **Lease or Property Documents:** If they are renting or owning property in Kenya, lease agreements or property ownership documents can also serve as address verification.
  - **Letter of Reference:** A letter from the customer's home country bank or financial institution may also serve as address verification or evidence of previous banking history.

3.4.2 The Obligation to Identify and Verify the Identity of a Person Acting on behalf of the Customer and to ensure they are so authorized

One of the key CDD requirements is to identify and verify the identity of a person acting on behalf of a customer and to confirm that the person is authorized to act on behalf of the customer.

Step 1: Obtain Documentary Proof of Authorisation:

The FI must verify that the person has been explicitly authorized to act. Acceptable documents that can be used to verify the authorisation include:

- Power of Attorney (PoA): A notarised or registered document granting the person legal authority to act on behalf of a customer.
- Board Resolution: (for customers that are legal persons) stating that the individual has been appointed to act on behalf of the entity.
- Letter of Authorisation: Signed by the customer or legal entity, specifying the scope and duration of authority.

- Partnership Agreement / LLP Deed: Specifies roles and who can act on behalf of the firm.
- Trust Deed or Trustee Resolution: If dealing with a trust, confirm the individual is a trustee or an appointed agent.

Step 2: Subject Authorised Person to complete CDD measures. The person acting on behalf of the customer must be subject to CDD checks.:

Step 3: Assess the legal capacity of the person acting on behalf of the Customer

- Ensure the person acting on behalf of the customer has the legal capacity act on behalf of the customer (e.g. not a minor or mentally incapacitated, etc.).
- Check that the person is not restricted or subject to court injunctions or regulatory bans.

3.4.3. Requirement to establish ultimate beneficial ownership

One of the key CDD requirements highlighted under Regulation 22 is the obligation for FIs to establish beneficial ownership of a customer that is a legal person or legal arrangement.

Regulation 22 states that…

22. *(1) A reporting institution shall identify and verify the natural persons behind a legal person and legal arrangement.*

(2) A reporting institution shall understand the nature of business, ownership and control structure when performing customer due diligence measures in relation to a customer that is a legal person or legal arrangement.

(3) In fulfilling the obligations under sub- regulations (1) and (2), a reporting institution shall obtain the following, where applicable—

(a) details of incorporation or registration;
(b) partnership agreement;
(c) deed of trust;
(d) particulars of directors and shareholders;
(e) names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement;
(f) names of the trustees, beneficiaries or any other natural person exercising ultimate effective control over the trust;
(g) any other documentation obtained from a reliable obtained from a reliable independent source proving the name, form and current existence of the customer.

(4) The relevant identification data in sub-regulation (3) may be obtained from a public register, the customer or other reliable sources.

For additional clarification regarding beneficial ownership refer to the Guidance on Beneficial Ownership (BO) issued by CBK.

3.5 Obligation for to understand the nature and purpose of transactions

FIs are obligated to take steps to understand the nature and purpose of the intended transaction or business relationship. This helps assess the risk associated with a customer and detect suspicious activity. Here are the key steps involved:

Step 1: Obtain Information from the Customer

- The reasons for opening the account.
- Why they intend to use particular financial products and services.
- The kind of transactions they intend to carry out and how frequently they expect to transact and in what amounts.
- Who they will be transacting with (e.g. suppliers, clients, beneficiaries).
- What the source of funds will be (e.g., salary, business income, inheritance).
- Will the transactions include cross-border transactions to jurisdictions rated to be a high risk of ML/TF/PF.

This information can be obtained using:
- Customer onboarding forms.
- CDD/KYC questionnaires.
- Interviews conducted by relationship managers/tellers.

Step 2: Review of Supporting Documents

Verify the customer's stated purpose with documentation, such as:
- Employment contracts (for salary earners).
- Business registration documents and invoices (for companies).
- Trust deeds or investment agreements (for legal arrangements).
- Loan agreements, property sale contracts, etc. (for specific large transactions).

3.6 Obligation to conduct On- going Due Diligence

Regulation 34 and 35 specify the measures that FIs are required to undertake to conduct ongoing due diligence:

34. *(1) A reporting institution shall monitor the business or account activity and transactions of their customers on a continuous basis.*

(2) On-going monitoring of business or account activity and transactions may be conducted on a risk-sensitive basis.

(3) A reporting institution shall conduct on-going due diligence on its customers and develop risk based systems and procedures.

35. *A reporting institution shall conduct ongoing due diligence on the business relationship—*

(a) by scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) by 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.

3.6.1 Ongoing Due Diligence Measures

Ongoing due diligence is a critical component of the CDD process, that aims to ensure that FIs continuously assess and manage the risks associated with their customers throughout the business relationship. This involves:

(a) Regularly reviewing and updating customer information including:

- Identification documents such as ID and passports;
- Beneficial ownership details; and
- The purpose and intended nature of the relationship.

(b) Monitoring customer transactions to ensure that they are consistent with the institution's knowledge of the customer's business and risk profile.

On-going due diligence measures should be implemented on a risk-sensitive basis. This means that the process should establish a risk-based monitoring system that profiles customers based on the frequency with which the measures above in (a) and (b) should be conducted on a risk -sensitive basis. their risk level (low, medium, or high).

Higher-risk customers, such as politically exposed persons (PEPs), entities operating in high- risk jurisdictions, or those with complex ownership structures, are subject to more frequent reviews and more intensive monitoring. FIs should use manual or automated systems to detect unusual or suspicious activity, such as transactions that are unusually large, complex, or inconsistent with the customer's typical behaviour.

FIs need to take note that with regards to the review and updating of CDD records, Regulation 35 (b) requires that priority must be placed on updating CDD documentation for customers that pose a higher risk. This could include either a manual system or an automated system.

(a) For a manual system designed to support ongoing monitoring and updates to CDD information and risk profiles, the process entails:

i. **Assigning each customer a risk category based on factors such as** legal form, occupation, transaction patterns, and geographic risk.

ii. **Establishing a central manual register or spreadsheet that tracks each customer's risk rating, the last CDD review date, and the next scheduled review.** The frequency with which the documentation is reviewed is determined by risk level, as needed.

iii. **Conducting periodic reviews of the CDD documentation using standardized checklists,** ensuring updates to identity documents, employment status, source of funds, and contact information. Customers can be contacted via phone, email, or in person to confirm or collect updated documentation. All updates are logged with the date, reviewing officer's name, and summary of the changes. If a customer fails to respond or if inconsistencies are found such as a new business activity not previously disclosed, the case should be escalated to compliance for further assessment.

iv. **Manual transaction logs should be reviewed to identify unusual activity that might prompt a CDD update.** For example, a customer posing a lower risk suddenly receiving large international wire transfers would trigger an interim review to reassess their risk profile. These reviews are documented, and necessary updates are made to the customer's file and risk classification.

(b) An automated system that identifies customers whose CDD information needs to be updated by using a combination of predefined rules, risk-based triggers, and system alerts. This ensures compliance with CDD requirements and maintenance of accurate customer risk profiles. Examples of such systems are highlighted below:

i. **Scheduled Review Triggers:** A monitoring system programmed to prompt reviews based on how long it has been since the customer's last CDD update.

ii. **Risk-Based or Event-Driven Triggers:** The system identifies customers for CDD updates when certain events occur, such as:

- Unusual or large transactions inconsistent with the customer's profile.

- Changes in personal or account information, such as address, phone number or occupation.
- Addition of a new signatory or change in beneficial ownership.
- Involvement in high-risk transactions or jurisdictions.
- Becoming a Politically Exposed Person (PEP).
- Negative news or sanctions screening hits.

iii. Dashboard Alerts and Reporting: Automated systems generate reports or dashboards indicating:

- Customers with overdue CDD reviews.
- Upcoming CDD review deadlines.
- Customers with missing or expired documents (e.g., ID or business license).
- Risk rating changes that require updated information.
- Compliance or relationship managers are alerted via the system to initiate contact with customers or request updated documents.

iv. Document Expiry Monitoring: A system that tracks the validity of submitted documents, such as national IDs, passports, or business registrations. When a document is about to expire (e.g., within 30–60 days), the system sends alerts or auto-emails to both the institution and the customer.

3.6.2 The Risk - Based Approach to CDD

Regulation 7 requires FIs to take appropriate steps to conduct a comprehensive risk assessment to effectively identify, assess, understand, monitor, manage, and mitigate ML/TF/PF risks.

When carrying out this risk assessment, FIs must:

i. Document all risk assessments and maintain records of the risk assessments.
ii. Evaluate all relevant risk factors, including:
    - The nature of customers,
    - Geographic locations (countries or regions),
    - Products and services offered,
    - Nature of transactions, and
    - Delivery channels .

Based on the Risk Based Approach (RBA), a risk assessment framework should be used to identify which customers present a higher or lower risk. This is in order to determine the level of CDD measure to be applied. Where a customer is assessed as posing a lower risk then simplified due diligence (SDD) measures are to be applied. Where a customer is assessed as posing a higher risk, then enhanced due diligence (EDD) measures are to be applied.

3.6.3 Assessing Customer Risks

Assessing customer risk is a fundamental component of an effective ML/TF/PF risk management framework. It enables FIs to determine the appropriate level of scrutiny and ongoing monitoring required for each customer. By developing a comprehensive customer risk profile, FIs can identify potential exposure to ML/TF/PF and other illicit activities.

This risk-based approach allows institutions to apply proportionate and targeted mitigating measures, ensuring that higher-risk customers are subject to enhanced due diligence, while lower-risk customers are managed appropriately within a simplified or standard due diligence framework.

3.6.3.1 Customer Risk Factors

When assessing customer risk, FIs are expected to consider multiple risk factors including:

i. **Customer Type:** Determine whether the customer is a natural person, legal person or legal arrangement, as certain customer types may pose higher risks (e.g., politically exposed persons (PEPs) or high-net-worth individuals.

ii. **Ownership Structure:** Determine the ownership structure of a customer to ensure transparency, particularly in the case of complex corporate structures or entities with multiple layers of ownership.
   - **Nature of Business or Occupation:** Evaluate the customer's industry or sector to identify any sectors that are more prone to money laundering, terrorist financing, proliferation financing or other financial crimes (e.g., casinos, real estate, arms dealing or offshore services.

iii. **Products and Services:** When assessing a customer's Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF) risk, FIs must consider the products and services the customer will be using because certain products and services inherently carry higher or lower levels of risk. FIs must evaluate how likely a product or service is to be misused for ML/TF/PF purposes. This involves identifying:
   - **Higher-risk products/services:** Those that offer anonymity, rapid movement of funds, or cross-border transfers.
   - **Lower-risk products/services:** Those with strong controls, low transaction volumes, or limited use.

   Certain features increase the ML/TF/PF risk of a product or service, such as:
   - Ease of anonymous use (e.g., prepaid cards, crypto-assets).
   - Cross-border accessibility (e.g., international wire transfers).
   - Volume and velocity of transactions.
   - Cash intensity (e.g., cash deposits or withdrawals).
   - Complexity of the product (e.g., trade finance, private banking).

iv. **Delivery Channel:** Assess the ML/TF/PF risks associated with a delivery channel, by evaluating how the customer would accesses its services—whether face-to-face, online, through agents, or other means. The FIs should consider factors such as the level of identity verification, degree of customer anonymity, control over the process, and exposure to high-risk jurisdictions. Channels that offer less transparency or allow remote access without strong verification generally pose higher ML/TF risks.

Table 4: Delivery Channel - Risk Factors

Factor	Risk Consideration
Face-to-face	Lower risk due to strong verification
Digital/online	Medium to high risk if not properly verified
Third-party introducers	Higher risk if introducer is unregulated or offshore
Agents	Varies – depends on oversight and verification
Mobile/digital wallets	Higher risk if unregulated

v. **Geographic/Jurisdiction Risk:** FIs would be expected to consider the following factors:

   - Assess the customer's country or region, considering whether it is a high-risk jurisdiction, such as one with weak AML/CFT/CPF controls either on the FATF blacklist or grey list or the EU list of third countries for money laundering.
   - Consider whether the customer's business involves doing business with entities located in jurisdictions that have been publicly identified as high risk-jurisdictions.

vi. **Source of Funds and Wealth:** Understand the origin of the customer's funds and wealth to ensure they are legitimate. Unclear or suspicious sources may indicate a higher risk.

vii. **Transaction History:** Review the customer's historical transactions to detect patterns that could indicate suspicious behaviours or a higher likelihood of engaging in illicit activities. For new customers, collect information on the nature and size of transactions that the customer will engage in. Consider the size, frequency and complexity of transactions that the customer is expected to conduct. Large or complex transactions may pose a higher risk.

viii. **Sanctions and Watchlists:** Check whether the customer, or their associated parties, appear on any sanctions lists or are subject to international or national restrictions.

ix. **Third-Party Risk:** Consider the involvement of third parties in the customer's transactions, particularly if there is no clear explanation for their role or if they are located in high-risk jurisdictions.

FIs are further advised to refer to the inaugural Report on the National Risk Assessment on Money Laundering and Terrorism Financing (NRA) Report of 2021 and other subsequent updates. The report can be accessed at the FRC website on the following link:

https://www.frc.go.ke/wp-content/uploads/2024/02/Update-on-NRA-of-ML-1-1.pdf

3.6.3.2 Customer Screening

FIs carry out initial screening prior to onboarding new customers or engaging in an occasional transaction. Thereafter, ongoing screening is required throughout the course of the customer relationship. Prospective customers should be screened against the following key lists:

i. Sanctions Lists issued under United Nations Security Council Resolutions (UNSCRs).

These lists can be accessed at UN Security Council Consolidated List which is a single, comprehensive list maintained by the United Nations that identifies individuals and entities subject to sanctions imposed by the UN Security Council.

https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list

- FIs should screen customers against sanctions lists issued by the UN Security Council Resolutions, which include individuals, entities, and countries subject to targeted financial sanctions related to terrorist financing and proliferation financing.
- TF and PF regulations require that FIs in the event that a customer is found to be sanctioned by the UN should take the following actions:

(a) Not proceed with the transaction or establish a business relationship with the customer.
(b) File a suspicious transaction report (STR) with the Financial Reporting Centre (FRC).

FIs are advised to refer to the Guidance Note on Targeted Financial Sanctions issued by the FRC.

Targeted financial sanctions related to terrorism financing

- UNSCR 1267 The ISIL (Da'esh) and Al-Qaida Sanctions List: This list targets individuals and organizations associated with terrorist groups like Al-Qaida, ISIS, and others, subject to financial sanctions and asset freezes.

https://main.un.org/securitycouncil/en/sanctions/1267/aq_sanctions_list

- UNSCR 1373 - Domestic list issued by the Inter-Ministerial Committee that is posted on the FRC website.

https://www.frc.go.ke/?p=687

ii. Sanctions Lists issued by Countries/Regional Bodies: Many countries maintain sanctions lists of individuals or entities. These lists can vary depending on the country and jurisdiction in which the FI operates.

- European Union (EU) Consolidated List: The EU also maintains sanctions lists that include individuals, organizations, and countries subject to EU measures for various reasons, such as terrorism financing or involvement in conflicts.

https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en

- The US Department of Treasury Office of Foreign Assets Control (OFAC) Sanctions List: This list includes individuals, entities, and countries subject to U.S. sanctions due to involvement in activities like terrorism, narcotics trafficking, or human rights violations.

https://sanctionslist.ofac.treas.gov/Home/ConsolidatedList

- His Majesty's Treasury (HM Treasury) United Kingdom (UK):

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

iii. Politically Exposed Persons (PEP) Databases: FIs must screen customers against PEP lists to identify individuals (both foreign and domestic) who hold or have held prominent public functions (e.g., government officials, senior politicians, judges, military leaders).

PEPs represent a higher risk due to the potential for corruption, bribery, or other illicit activities. FIs are required to also screen the close family members and associates of PEPs.

For additional information refer to CBK's Guidance on Politically Exposed Persons (PEPs).

iv. Global Adverse Media Screening: FIs should screen customers for any negative news or media reports indicating involvement in financial crimes, fraud, corruption, or other illicit activities. There are commercial databases and third-party services that provide screening of global media sources for adverse information related to a customer.

3.6.3.3 Assigning Risk Ratings

FIs assign ML/TF/PF risk ratings to customers as part of their risk-based approach to compliance and due diligence. This classification is determined by evaluating various risk factors, including the customer's nature of business, geographical location, transaction behaviour, source of funds, and ownership structure.

3.6.3.4 Simplified Due Diligence

Regulation 21 allows a FI to apply simplified due diligence (SDD) measures under specific conditions:

- When a customer has been identified as presenting a lower risk. The FI must conduct an adequate risk analysis to identify situations where risks are deemed low.
- The simplified measures must align with the identified lower risks, ensuring that the level of due diligence is proportionate to the assessed level of risk.

Simplified due diligence cannot be applied in cases where there is any suspicion of money laundering, terrorism financing, or proliferation financing. Additionally, SDD measures are not permitted when the situation involves specific higher-risk scenarios, ensuring that the institution still addresses potential risks effectively in such cases.

Key considerations when applying the simplified due diligence measures:
- Apply only in cases of proven low-risk .
- CDD requirements must adhere to the minimum CDD requirements set out under the POCAMLA and POCAML Regulations whether the customer is a natural person, legal person or legal arrangement.
- Document and justify all SDD decisions
- Escalate to enhanced due diligence if higher risk is proven.

Examples of simplified due diligence include:

- Basic ID Verification
  Use of basic identification documents that meet the minimum requirements spelt out under the POCAMLA and POCAML Regulations.
- Product Restrictions to Control Risk
  - Offer products with limited functionality (e.g., low-value prepaid cards)
  - Products and services that do not permit higher-risk features (e.g., cross-border transactions)
- Reduced Frequency of CDD reviews
  - Customer due diligence (CDD) reviews over longer intervals.
  - Applicable only to stable, low-risk customer profiles

3.6.3.5 Enhanced Due Diligence (EDD)

Regulation 20 requires FIs to apply EDD when a customer or entity presents a higher ML/TF/PF risk .

Key EDD measures include:
i. Obtaining additional information to establish the customer's identity.
ii. Applying extra verification checks on submitted documents.
iii. Obtaining senior management approval prior to establishing or continuing the relationship.
iv. Verifying the source of funds.
v. Conducting ongoing monitoring of the business relationship.

For identified higher risks (at a national, sectoral, or institutional level), FIs must:

i. Apply enhanced measures to mitigate those risks, or
ii. Incorporate the identified risks into their internal risk assessments.

For legal persons or arrangements determined to be higher risk, FIs must take reasonable steps to identify and verify the beneficial owner before making any payout.

FIs should ensure that EDD is mandatory for customers wherever higher risks of ML/TF/PF are identified.

PART IV. OTHER RELATED CDD MEASURES

4.1. Eligible Introducers

Eligible introducers for the purposes of conducting CDD, are individuals or entities that are legally recognized and authorized to introduce a customer to an FI, ensuring that the customer's identity and relevant information have been properly verified before the relationship is established.

Eligible introducers are responsible for verifying the identity of the customer and ensuring that the relevant due diligence procedures are followed before introducing the customer to the financial institution. They provide a level of assurance that the customer has been sufficiently identified, and their risk profile has been assessed, helping to streamline the CDD process while ensuring compliance with legal and regulatory requirements

Eligible introducers are typically subject to AML/CFT/CPF regulatory requirements and can include:

(a) Regulated FIs: Other FIs such as banks, insurance companies, or investment firms that are already subject to AML, CFT and CPF requirements and have conducted their own CDD processes on the customer.
(b) Lawyers or Notaries: Legal professionals who are regulated and can verify the identity of their clients as part of their legal services, ensuring that the customer meets the necessary CDD requirements.
(c) Accountants or Auditors: d accountants or auditors who are regulated and can provide information about the customer's identity and financial standing.

4.2 Group Wide Programmes

Regulation 28 requires financial groups to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group:

(a) policies and procedures for sharing information required for the purposes of CDD and ML/TF/PF risk management;
(b) the provision, at group-level compliance, audit and/or AML/CFT/CPF functions, of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done) Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and
(c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

4.3 Politically Exposed Persons (PEPs)

The FATF Recommendation 12 has defines Politically Exposed Persons (PEPs) to mean:

- Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
- Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
- Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

FIs should ensure that they adopt appropriate risk management systems to determine whether a custom or an account holder or a beneficial owner is a politically exposed person or PEP.

For CDD requirements for PEPs refer to Guidance Note on PEPs issued by CBK.

4.4 CDD for Beneficiaries of Life Insurance Products

In addition to the CDD measures required for the customer and the beneficial owner, Regulation 24 requires FIs to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated:

(a) for a beneficiary that is identified as specifically named natural or legal persons; or legal arrangements – taking the name of the person;
(b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the payout;
(c) For both the cases outlined in (a) and (b), the verification of the identity of the beneficiary should occur at the time of the payout.

FIs are also required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If the FI determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it should be required to take EDD measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

4.5 Third Party Reliance

Regulation 33 permits FIs (FIs) to rely on third parties to carry out elements of customer due diligence (CDD) or to introduce business, provided that the third parties meet the criteria set out in the POCAMLA Regulations. The FI should enter into an agreement outlining the responsibilities of each party.

It states that…

33. *(1) A reporting institution may rely on a third party to perform elements of customer due diligence measures, or to introduce business, provided that the institution meets the criteria set out in these Regulations.*

(2) A reporting institution relying on a third party shall enter into an agreement with the third party outlining the responsibilities of each party.

It should be noted, however, that where an FI places reliance on a third party, the FI remains ultimately responsible for ensuring compliance with the CDD requirements under POCAMLA and the POCAMLA Regulations. The third party is not accountable for meeting these obligations.

Regulation 33(9) defines a third party …..

(9) For purposes of this regulation, the term "third party" means another FI or designated non-financial business or profession or a person that is supervised or monitored by a competent authority.

For an FI to rely on a third party, the FI should ensure that the third party meets the following criteria:

(a) An FI relying upon a third party should immediately obtain the necessary information concerning of the CDD measures
(b) An FI should take adequate steps to satisfy themselves that upon request, copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
(c) An FI should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements in line with the POCAML and POCAML Regulations.

FIs should note that the elements of CDD that an FI can rely on a third party to provide as stipulated in the FATF Recommendations include:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
(b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the FI is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include understanding the ownership and control structure of the customer.
(c) Understanding and obtaining information on the purpose and intended nature of the business relationship.

4.5.1. Reliance on a third party located in a foreign jurisdiction

Regulation 33(7) requires that when an FI places reliance on a third party that is in a foreign country, the FI should assess the ML/TF/PF risks that the country poses and the adequacy of CDD measures adopted by reporting institutions in that country.

4.5.2. Reliance on a third party that is part of the same financial group

Where an FI relies on a third party that is part of the same financial group to perform elements of CDD, or to introduce business, Regulation 33(8) requires the FI to ensure that the requirements of this regulation are met in the following circumstances —

(a) the group applies CDD and record-keeping requirements and AML/CFT/CPF measures.
(b) the implementation of CDD, record keeping requirements and AML/CFT/CPF programmes are supervised at a group level by a competent authority; and
(c) any higher country risk is adequately mitigated by the group's AML/CFT/CPF policies.

PART V. CUSTOMER DUE DILIGENCE EXCEPTIONS AND PROHIBITED PRACTICES

5.1 When a Financial Institution is unable to comply with CDD Requirements

Regulation 25 (2) requires that where a customer is unable to provide evidence to support CDD requirements including beneficial ownership then the FI is required to:

(a) not open the account;
(b) not commence any business relationship with the customer;
(c) not perform the transaction;
(d) where it has commenced a business relationship with the customer:
i. discontinue any transaction it is conducting for him or her.
ii. bring to an end the business relationship or any understanding it has reached with him or her.
(e) file a suspicious transaction report with the FRC.

5.2 When there is a Suspicion of Money Laundering of Terrorism Financing

Regulation 25(6) states that where a FI forms a suspicion of money laundering or terrorism financing, and it reasonably believes that performing the CDD process will tip off the customer, the FI is permitted to not continue with the CDD process and instead file a suspicious transaction report (STR) with the Financial Reporting Centre (FRC).

5.3 Prohibition on Dealing with Shell Banks

Regulation 30 (1) prohibits an FI from opening a foreign account with a shell bank or permitting its account to be used for correspondent banking with a shell bank.

It states that …
1) A reporting institution shall not have dealings with shell banks;
(a) open a foreign account with a shell bank;
(b) permit its accounts to be used by a shell bank; or
(c) enter into or continue a correspondent financial relationship with—
(i) a shell bank; or
(ii) a respondent FI that permits its account to be used by a shell bank."

The FATF defines a shell bank to mean "a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision". Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute a physical presence.

Shell banks present significant AML/CFT/CPF risks because they are easily used for money laundering and hiding the origins of funds. They lack physical offices, employees, and genuine business activities, making it difficult to verify their legitimacy and ownership. This lack of transparency allows illicit actors to mask the true owners of assets or property derived from criminal activity, making them vulnerable to abuse.

5.4 Prohibition on Opening Anonymous or Fictious Accounts

Regulation 13(1) prohibits reporting institutions that is, all FIs or DNFBPs from opening or maintaining anonymous or fictitious accounts. In considering this prohibition, it is critical for FIs to distinguish between anonymous fictious accounts and numbered accounts.

- An anonymous or fictitious account is one that is opened without disclosing the true identity of the account holder, often using a false name or identity. These accounts provide extreme privacy but are highly susceptible to misuse for illegal activities like money laundering or tax evasion. Anonymous accounts lack transparency and traceability, making them illegal and non-compliant.
- A numbered account is a type of an account where the client's name is replaced by a number or code to provide a higher level of confidentiality. While the identity of the account holder is known to the FI, it is restricted to a small group of senior officials. These accounts are typically used by high-profile individuals or corporations seeking privacy, and they are legal. Numbered accounts are used to maintain financial discretion in private banking.

5.5 Tipping Off

Section 8 of POCAMLA states that

"(1) A person who—
(i) knows or ought reasonably to have known that a report under section 44 is being prepared or has been or is about to be sent to the Centre;
and
(ii) discloses to another person information or other matters relating to a report made under paragraph (i), commits an offence.
(2) In proceedings for an offence under this section, it is a defence to prove that the person did not know or have reasonable grounds to suspect that the disclosure was likely to prejudice a report made under subsection (1).
(3) For the purposes of this section, a "person" includes a financial group.

While Regulation 8 of the POCAML Regulations states that

"A reporting institution which obtains information which is suspicious or indicates possible money laundering, terrorism financing or proliferation financing activity shall not disclose such information to an unauthorised person but shall report it to the Centre as required by these Regulations."

Best practices that Fis could adopt include:

- Restrict STR-related communication to authorised personnel.
- Label STRs as "confidential" in internal systems.
- Use secure channels for filing STRs.
- Train frontline and operational staff on:
  - What constitutes suspicious activity.
  - The importance of non-disclosure.
- Have documented policies on managing STRs discreetly.

PART VI. RECORD KEEPING

Financial institutions are required to retain all documentation obtained during the CDD process for a minimum period as stipulated in the POCAMLA and POCAML Regulations (currently 7 years), from the date of the transaction or the end of the business relationship. This includes copies of identification documents, beneficial ownership information, and any other data used to verify the customer's identity.

In addition, financial institutions must ensure that the records:

- Are readily available to competent authorities, including the FRC and other law enforcement/ investigative agencies, regulators and supervisors upon request.
- Must be maintained in a manner that allows for easy access and retrieval to facilitate timely investigations, audits, and regulatory examinations related to money laundering, terrorist financing, proliferation financing or other financial crimes.

PART VII. CONCLUSION

The effective implementation of Customer Due Diligence (CDD) measures is critical to safeguarding the integrity of Kenya's financial system and ensuring compliance with the framework established under the POCAMLA) and its regulations.

FIs are expected to adopt a risk-based approach to CDD, ensuring that the extent of due diligence applied is proportionate to the level of risk presented by each customer or transaction. This involves the proper identification and verification of customers, understanding the nature and purpose of the business relationship and conducting ongoing monitoring. FIs must also remain vigilant in applying EDD where higher risks are identified and ensure that CDD information is kept up to date. Consistent adherence to these measures will further strengthen institutional resilience against money laundering, terrorism financing, proliferation financing, and related financial crimes.

PART VIII. EFFECTIVE DATE

The effective date of this Guidance shall be September 1, 2025.

PART IX. ENQUIRIES

In the event of any clarifications or enquiries on any aspect of this guidance should be referred to:

Director,
Bank Supervision Department
Central Bank of Kenya
P. O. Box 60000 – 00200
NAIROBI
Tel: +254-20-2860000 Email: fin@centralbank.go.ke

ANNEX

Legal Entities Registered at the Business Registration Service (BRS)

Type of Legal Structure	Type of Entity	Definition
Legal Persons	Private Limited Company	A company is limited by shares if the liability of its members is limited by the memorandum to the amount, if any, unpaid on the shares respectively held by them. A private company is also a company that is restricted from inviting the public to subscribe to its shares. The membership of a private limited company is restricted to a maximum of 50 members.
	Public Limited Company	A public limited company allows its members the right to transfer their shares in the company and the articles do not prohibit invitations to the public to subscribe for shares or debentures of the company. The name must end with the expression “Public Limited Company” or the abbreviation “PLC”.
	Company Limited by Guarantee	A company limited by guarantee (CLG) is an alternative type of corporation used primarily for non-profit organizations that require legal personality. This type of company does not have share capital and its members are guarantors rather than shareholders. The liability of members is limited to the amount they agree to contribute to the company’s assets if it is liquidated.
	Limited Liability Partnerships (LLPs)	Limited liability partnerships commonly referred to as LLPs are unique forms of business association that combines elements of a company with those of a partnership. Upon registration, an LLP becomes a body corporate with a legal personality separate from its partners.
	Foreign Company	This type of a company is a branch of a company registered outside of Kenya, that has established a place of business in Kenya.
Legal Arrangements	Trust	A trust is a fiduciary relationship where a settlor (person setting up the trust) gives another party, known as the trustee, the right to hold title to property or assets for the benefit of a third party commonly referred to as beneficiaries.

Central Bank of Kenya

Haile Selassie Avenue P.O. Box 60000 - 00200 Nairobi |Tel: (+254) 20 - 286 0000 / 286 1000 / 286 3000