

Customer Due Diligence: Fundamentals & Emerging Concepts

Brought to you by:



Introduction to The AML/CFT Mission



To combat financial crimes through the implementation of strong AML/CFT measures;

To protect the international and Emirati financial systems from criminal abuse; and

To combat threats to national, regional, institutional, and collective security through increased transparency and the application of financial sanctions and other efforts.



ROADMAP

For Today's Discussion

Foundations of an Internal AML/CFT Core Framework

Customer Due Diligence

- Overview and Global Standards
- CDD: Program and Elements
- Enhanced Due Diligence
- Key Considerations for Entities

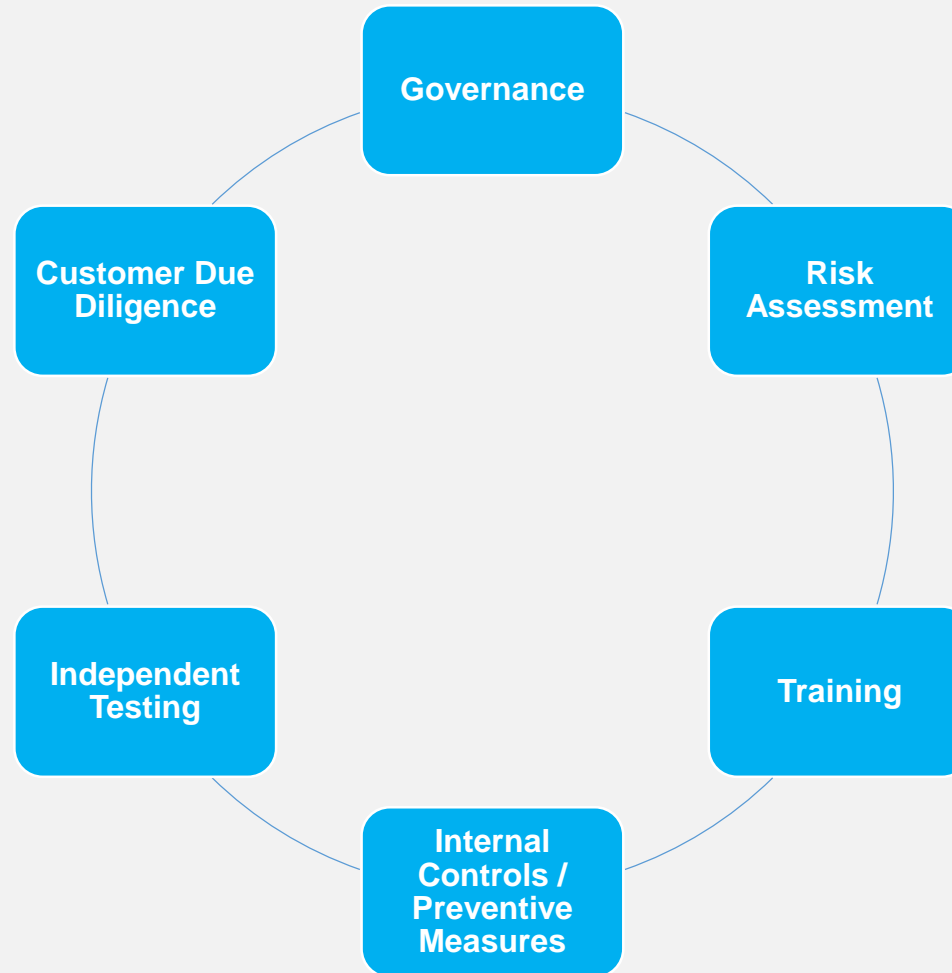
Emerging Concepts

Fact Pattern and Discussion



Foundations of an Internal AML/CFT Core Framework

The Key Elements



Customer Due Diligence Overview



A robust CDD program allows an institution to understand and assess the risk associated with its customer, as well as the customer's expected and usual banking practices, so that the institution can manage risk and detect and report unusual or potentially suspicious customer activity.



Customer Due Diligence

Global Standards and Expectations



**The Financial
Action Task
Force (FATF)**



**Middle East and
North Africa
Financial Action
Task Force
(MENAFATF)**



**The United Arab
Emirates**



**Foreign Financial
Centres and
Foreign
Correspondent
Relationships**



Customer Due Diligence

CDD Program Overview

An effective CDD Program includes four essential elements:

- **Customer identification and verification;**
- **Beneficial ownership identification and verification;**
- Understanding the **nature and purpose of customer relationships and accounts** to establish expected customer and account activity and related risk profiles; and
- **Ongoing monitoring** for detecting unusual activity, reporting suspicious transactions, and, on a risk basis, updating customer information (e.g., through the periodic risk assessment process).

If unable to complete CDD, the entity should not open the account, commence business relations, or perform the transaction—or should terminate the business relationship.

Effective CDD also requires specific and **enhanced due diligence (EDD)** to be performed on higher-risk customers.



Customer Due Diligence

Customer Identification and Verification

CDD begins with customer identification and verification—using reliable, independent source documents, data, and information—which enables an entity to form a reasonable belief about the true identity of each of its customers, including by:

- Obtaining specified identifying information (including name, address, government identification number, and, for individuals, date of birth) from each customer; and
- Verifying the accuracy and validity of the identifying information obtained via documentary methods (such as an unexpired government ID or certified articles of incorporation) and/or non-documentary methods (such as a commercial database).

The entity should also develop a customer risk profile based on factors such as customer type, products used, account transactions, product and services and geography.



Customer Due Diligence

Beneficial Ownership Identification and Verification

Beneficial ownership includes the natural persons who :

- who ultimately have a controlling ownership interest in a legal person, depending on the ownership structure of the legal person and potentially subject to a minimum ownership threshold (e.g. 25%)
- Exercise control of the legal person or arrangement through other means, when there is doubt under as to whether the natural person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests
- Holds the position of senior managing official, when no natural person ultimately has a controlling ownership interest or exercises control of the legal person or arrangement through other means.
- For trusts, 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

Necessary information can be obtained from a public register, from the customer, or from other reliable sources.

An entity should take reasonable measures to verify the beneficial owner's **identity**, rather than that person's **status** as beneficial owner.

Efforts should be undertaken to understand the control structure of legal persons and arrangements



Customer Due Diligence

Nature and Purpose of the Relationship

In order to understand the nature and purpose of a customer's account and relationship an entity should obtain:

- An understanding of the customer's account activity and the types of products and services used or anticipated;
- The reason and purpose for establishing the customer relationship;
- The actual or anticipated source of the initial deposit, if there is a deposit relationship;
- Information about the customer's employment (for individuals) or business (for legal entities);
- Primary trade areas and information concerning major suppliers and customers, as applicable;
- Geographic information, such as the customer's location and the locations of where the customer transacts business or has significant operations; and
- For preexisting customers, information regarding any material changes in the customer relationship over time.

Based on this information, the entity should determine whether the customer's source of funds and products/services are consistent with what the entity knows about the customer and its business or occupation.



Customer Due Diligence

Ongoing Monitoring and CDD Updates

Conducting ongoing due diligence on the relationship and scrutiny of transactions throughout the course of that relationship to ensure activity is consistent with the entity's knowledge of the customer.

To do this, a customer's information should be updated as part of periodic reassessment and in response to certain events and as a result of ongoing, risk-based monitoring and.

Periodic assessment requires that customer information be updated according to risk rating. For example: High Risk – 12 months; Medium Risk – 24 months; Low Risk – 36 months.

Trigger events can include:

- An existing customer opening a new account;
- A material change to customer information;
- The discovery of any information that would reasonably call into question the reliability of beneficial ownership information; and
- The identification of adverse media on the customer.



Customer Due Diligence

Specific and Enhanced Due Diligence

In general, EDD measures can serve to:

- Clarify a customer's identity and activities in order to distinguish actual from apparent financial crime risks;
- Provide information that is material to ongoing monitoring of the customer's activities and additional data that is useful in assessing and resolving alerts;
- Provide information that justifies imposing restrictions and special conditions on high-risk client activity; and
- Identify customers who should be exited based on financial crime risk.

Relevant EDD information collected may include, for example:

- The customer's source of funds or wealth;
- Additional individuals with ownership or control over the customer relationship;
- The customer's occupation or type of business and domicile of business;
- Customer's primary trade area and whether international transactions are expected to be routine; and
- The customer's business operations, total sales (where applicable), anticipated volume of currency, transaction activity through the bank, list of major customers and suppliers, and explanations for increases in customer activity.



Customer Due Diligence

Key Considerations for Entities

- Comprehensive and clear AML/CFT core framework that includes:
 - Risk appetite statement based on business strategy;
 - AML/CFT controls that are matched to inherent risks of business and risk appetite;
 - Policies and procedures that cover full scope of business;
 - Systems and controls that implement those policies and procedures;
 - Independent audit function that ensure that policies and procedures are implemented and operating as intended.
- CDD is a cornerstone of an AML/CFT framework.
 - CDD is an enterprise-wide responsibility—across all lines—but first line owns the risk and responsibility for current, accurate, and complete CDD information
 - Four elements must work together—robust onboarding and robust monitoring
 - CDD program should drive risk management
- Ensuring adequate understanding of and commitment to the AML/CFT mission, including the reliance on a robust CDD program



Emerging Concepts

New Technologies, Virtual Assets, and Digital Identity

New payment technologies—including stored value (prepaid) cards, mobile banking platforms, and virtual currencies—are increasingly used as alternatives to traditional payment and money transmission systems.

These technologies have the potential to reduce the costs and increase the **speed** and **convenience** of funds transfers.

But these same features—combined with the increased opportunities for **anonymity**, **irreversible settlement**, and unmediated **peer-to-peer transactions**—introduce additional illicit financing risks that financial institutions must carefully assess and mitigate.



Fact Pattern & Discussion



Fact Pattern

Hypothetical Scenario

You are a compliance officer at Bank ABC, licensed by ADGM.

Your transaction monitoring system has alerted your team on a series of transactions related to a bank customer, Fletcher LLC. The alert was triggered by excessive volume of transactions and amounts with high-risk jurisdictions.

Upon review of the alerted transactions, you see payments involving Sudanese and Iraqi counterparties for undisclosed "services," including numerous round-dollar payments exceeding USD100,000 and totaling more than USD3,000,000 in the past three months.

You request the CDD file and the transaction history for the account. In the file you learn that Fletcher LLC is an international financial consulting company and the beneficial owner is John Smith Esq, a partner at Smith & Jones LLP's office in Cyprus. Smith & Jones LLP is also licensed by ADGM with a local office.

