



UNITED ARAB EMIRATES
MINISTRY OF ECONOMY

**ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM
AND ILLEGAL ORGANISATIONS**

**Implementation Guide For
DNFBPs on
CUSTOMER DUE DILIGENCE (CDD)**

**December, 2024
Version 0.3.2.1**

Customer Due Diligence (CDD)

Introduction:

The degree of money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risk that DNFBPs' customers face is dynamic and subject to fluctuation over time based on a number of variables. These variables include the recognition and acceptance of their customers, the type of business they operate, and the results of continuous observation.

Customer due diligence plays a crucial role in maintaining the integrity of the financial system. it helps prevent financial crimes and protect businesses from reputational damage. Furthermore, CDD is more than just a legal necessity. Additionally, it gives companies insightful information about their customers, enabling them to decide wisely and forge closer bonds with them.

The process of assessing pertinent data about your customer gathered at the Know Your Customer (KYC) stage is known as Customer Due Diligence (CDD), Simplified Customer Due Diligence (Simplified CDD), and Enhanced Customer Due Diligence (Enhanced CDD). Conducting proper customer risk assessment (CRA) is considered essential to determining the level of due diligence the DNFBPs will take. Refer to the guidance on conducting customer risk assessments (CRA). ¹

The purpose of this document is to provide practical guidance to entities regarding customer due diligence. We provide it to assist entities with day-to-day compliance challenges and provide examples of international best practice.

This guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF") and industry best practices and does not place restrictions on the actions that DNFBPs must take to fulfill their statutory obligations under the current legal and regulatory framework.

This document should be read in conjunction with the by-law, the AML/CFT Law, and the MOE's AML/CFT Guidelines for Designated Non-Financial Businesses and Professions. The guidance cannot address every possible scenario and is not legal advice. It does not replace the AML/CFT Law or other relevant AML/CFT/CPF legislation applicable in the UAE. Firms remain responsible for compliance with relevant legislation.

The Ministry of Economy has created this document in consultation with the DNFBP's Working Group under the Public and Private Partnership Committee.

¹ <https://www.moec.gov.ae/en/aml>

Customer Due Diligence (CDD)

What is Customer Due Diligence (CDD)?

CDD (Customer Due Diligence) measures are processes that require DNFBPs to verify customer identities, understand the purpose of the relationship, monitor transactions, and keep customer information up-to-date to prevent financial crimes.

When CDD is required?

DNFBPs need to undertake CDD measures when:

Establishing business relations;(before or during the course of establishing a business relationship or opening an account; and before carrying out a transaction for a customer with whom you are not in an established business relationship)

Carrying out occasional transactions above the applicable designated threshold (AED 55,000), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;

There is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere; or

The DNFBP has doubts about the veracity or adequacy of previously obtained customer identification data.

What CDD measures include:

For all customers

DNFBPs need to:

- Identify the customer (whether permanent or occasional and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data).
- Verify that any person purporting to act on behalf of the customer is so authorized and identify and verify the identity of that person.
- To not enter into any business relationship with a Shell company.

- Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the DNFBPs is satisfied that it knows who the beneficial owner is.
- Understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.
- Conduct ongoing due diligence on the business relationship, including:

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

(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.

For legal persons and legal arrangements

For customers that are legal persons or legal arrangements, the DNFBPs need to:

- understand the nature of the customer's business and its ownership and control structure.
- identify the customer and verify its identity through the following information:
 - (a) The name, Legal Form and Memorandum of Association.
 - (b) Headquarter office address or the principal place of business; if the legal person or arrangement is a foreigner, it must mention the name and address of its legal representative in the State and submit the necessary documents as a proof.
 - (c) Articles of Association or any similar documents, approved by the relevant authority within the State.
 - (d) Names of relevant persons holding senior management positions in the legal person or legal arrangement.

Identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons, through the following:

For customers that are legal persons

For customers that are legal persons, DNFBPs need to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- (a) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person (25% or more); and

(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(c) Where no natural person is identified under (a) or (b) above, DNFBPs should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

For customers that are legal arrangements

For customers that are legal arrangements, the DNFBPs need to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- (a) 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/ownership);
- (b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

Timing of verification

DNFBPs need to 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.

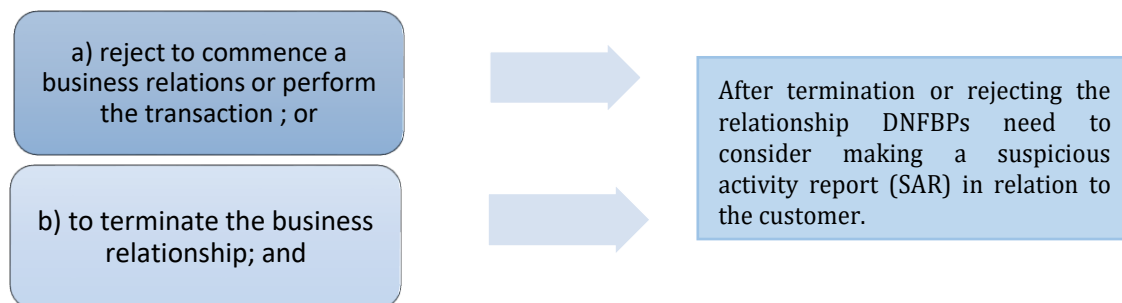
DNFBPs need to adopt risk management procedures with respect to the conditions under which a low risk customer may utilize the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

CDD requirements to Existing customers

DNFBPs need to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained

Failure to satisfactorily complete CDD

Where a DNFBP is unable to comply with relevant CDD measures:



The actions that will be taken by the DNFBPs need to be documented and available to be provided to the supervisory authority when requested.

CDD and Tipping-Off

DNFBPs (including their directors, officers, and employees) are prohibited from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the DNFBP is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

In cases where DNFBPs form a suspicion of money laundering or terrorist financing and they reasonably believe that performing the CDD process will tip-off the customer, they are permitted not to pursue the CDD process and instead to file an STR.

Reliance on Identification and Verification Already Performed

The CDD measures do not imply that DNFBPs have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. DNFBPs are entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile or historical transaction such as but not limited to (significant increases in transaction volumes, operations in new jurisdictions).

Ongoing Customer Due Diligence

DNFBPs are required to ensure 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.

Ongoing customer due diligence, or CDD, is the process of constantly monitoring and assessing customer relationships to ensure compliance with regulatory requirements and to mitigate risks associated with money laundering, fraud, and other financial crimes. This process typically involves:

- Regular Monitoring: Continuously reviewing transactions and customer activities to identify unusual or suspicious patterns.
- Updating Information: Regularly updating customer information, including identification details, to reflect any changes in risk profile.
- Risk Assessment: Assessing the risk level of each customer based on their behavior, transaction patterns, and the jurisdictions involved.
- Enhanced Due Diligence (EDD): Applying more rigorous measures for high-risk customers, such as additional documentation or scrutiny of transactions.
- Training and Awareness: Ensuring staff are trained to recognize red flags and understand the importance of ongoing CDD.
- Reporting: Complying with legal requirements for reporting suspicious activities to the appropriate authorities.

Ongoing CDD is crucial for maintaining the integrity of DNFBPs and ensuring they are not inadvertently facilitating illicit activities.

Generally, a Firm can rely on the CDD it has already undertaken unless it has doubts about the accuracy and reliability of that information, or it becomes out of date. However, CDD should be reviewed where there are doubts, for example if there is a suspicion of ML or TF, where there is a material change in the customer's account or business activity which is inconsistent with the customer's business profile.

Ongoing Customer Due Diligence need to be conducted on a recurring basis, depending on the risk associated with your client. 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”.

Record Keeping

All Firms operating in the UAE need to retain relevant CDD records for at least five years after the end of the business relationship. Records may be electronic and/or hard copy.

All documents and records obtained through CDD measures need to be kept. This includes: Copies or records of official identification documents such as passports, identity cards, driving licenses, or similar documents;

- Evidence of sanctions screening (at onboarding and on an ongoing basis);
- Account/registration files and business correspondence;

Analysis conducted by the Firm, such as inquiries to establish the background and purpose of complex, unusual large transactions.

The CDD records that need to be kept include all necessary records on transactions, both domestic and international, to enable a Firm to comply swiftly with information requests from Competent Authorities. These records need to be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for the prosecution of criminal activity.

General Considerations Regarding Documents

Information about a customer need to be verified using documents, data and information obtained from reliable and independent sources. This information should be current at the time it is obtained.

Documents should be clear and legible, including the photograph on customer identification documents.

The best documents to rely upon are those that are most difficult to counterfeit or obtain illicitly. This includes government issued identity cards, passports, reports from independent business and company registries, audited annual reports and other reliable sources of information.

When copy documents are relied on, they should be verified by an authorized staff member of the Firm sighting the original. Details of the verification should be recorded. If an original cannot be produced, the Firm may consider accepting a copy that is certified as a true copy by a notary public, lawyer or some other suitably qualified professional.

If a document is in a foreign language, the Firm should take appropriate steps, independent of the customer, to ensure that it understands the nature of the document and its content. This may be done by a staff member of the Firm conversant in the language providing a written summary of the key aspects of the document. Alternatively, a suitably qualified translator may be engaged by the Firm.

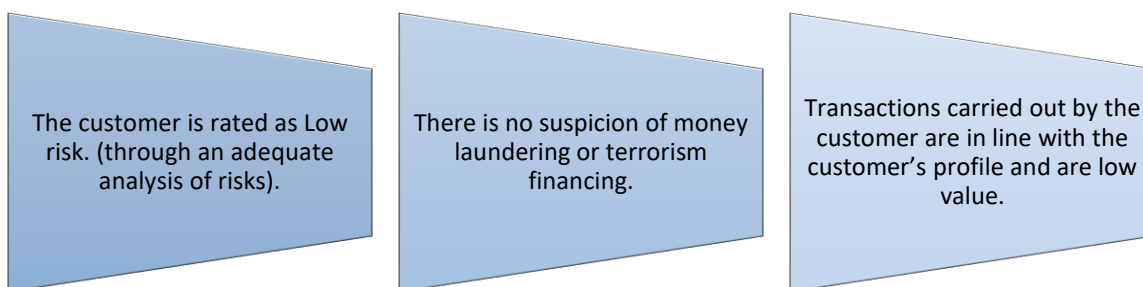
Simplified CDD and Enhanced CDD

Risk based Approach

DNFBPs need to perform enhanced due diligence where the ML/TF risks are higher. DNFBPs may only be permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country and the DNFBPs. The simplified measures should be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

When to conduct the simplified Due Diligence (“Simplified CDD”)

DNFBPs are permitted to apply simplified CDD when the customer meets the following criteria:



Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of ongoing transaction monitoring, based on a reasonable monetary threshold.
- Reducing the frequency of updating the Customer's information.
- Concluding the purpose and nature of the business relationship based on the type of transactions or the business relationship that has been established, without the need to gather information or performing specific procedure.
- Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.
- Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

What is Enhanced Customer Due Diligence (“Enhanced CDD”)

Enhanced CDD refers to applying higher standards for identification documents, a detailed evaluation of the purpose of establishing a business relationship, and increased monitoring of the ongoing business relationship. Enhanced CDD is generally applicable to customers, whose ML/TF risk was assessed as “High”, or where the customer or a beneficial owner of the customer is a PEP

When to conduct EDD?

EDD is typically required when a business relationship poses a higher risk of money laundering or terrorist financing. This may be due to the customer's location, their business activities, or their relationships with PEPs. By conducting EDD, businesses can better understand these risks and take appropriate measures to mitigate them.

Enhanced CDD refers to applying higher standards for identification documents, a detailed evaluation of the purpose of establishing a business relationship, and increased monitoring of the ongoing business relationship. Enhanced CDD is generally applicable to customers, whose ML/TF risk was assessed as “High”, or where the customer or a beneficial owner of the customer is a PEP.

DNFBPs should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, DNFBPs need to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

Examples of enhanced CDD measures that need to be applied for higher-risk business relationships include:

- Obtaining additional information on the customer and beneficial owners (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification information of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information/documents on the source of funds or source of wealth of the customer. (particularly for foreign PEPs)
- Obtaining information on the reasons for intended or performed transactions.
- 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 controls applied, and selecting patterns of transactions that need further examination.

Upon completion of Enhanced CDD on high-risk customers, senior management need to be involved in the decision making as to whether to onboard (or continue business relationship with) such customers. By involving senior management in the decision-making process, you ensure that all decisions are made in accordance with your firm's risk management policies and procedures and that senior management is fully aware of the potential risks associated with the customer.

Conclusion

In conclusion, CDD is a vital process that helps businesses manage risks and build stronger relationships with their customers. While it can be challenging, with the right approach and tools, businesses can conduct CDD effectively and efficiently.

As the financial landscape continues to evolve, the importance of CDD is likely to grow. Businesses that understand and embrace this process will be well-positioned to navigate the challenges and opportunities ahead.