مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

GUIDANCE FOR LFIs ON CUSTOMER DUE DILIGENCE / KNOW YOUR CUSTOMER AND RECORDKEEPING

06 November 2025

AML/CFT Supervision Department

CentralBankUAE
CentralBankUAE
Central Bank of the UAE
CentralBankoftheUAE
Central Bank of the UAE
المصرف–المركزي.امارات
www.centralbank.ae
Central Bank of the UAE:
Download on the App Store
GET IT ON Google Play
المصرف-المركزي.امارات
www.centralbank.ae

AGENDA

1. Purpose, Applicability and Legal Basis
2. Role and Significance of CDD/KYC and Recordkeeping
3. Customer Due Diligence
4. Recordkeeping
5. Q&A

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Purpose and Applicability of the Guidance

Purpose

- This Guidance does **NOT** constitute new regulation and does **NOT** introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- LFIs are expected to demonstrate compliance with requirements of the Guidance within one month from its coming into effect.

Applicability

The guidance document applies to **all natural or legal persons that are licensed and/or supervised by the CBUAE** in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, investment companies, payment service providers, virtual asset service providers ("VASPs"), payment token service providers, registered hawala providers;; and
- Insurance companies, agencies and brokers.

Legal Basis

- **Federal Decree-Law No. (14) of 2018**, Regarding the Central Bank & Organization of Financial Institutions and Activities, and its amendments ("CBUAE Law"). [repealed by Federal Decree-Law No. (6) of 2025, Regarding the Central Bank, Regulation of Financial Institutions and Activities, and Insurance Business]

- **Federal Decree Law No. 20 of 2018** on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended ("AML-CFT Law"). [repealed by Federal Decree-Law No. 10 of 2025 on Combating Money Laundering, the Financing of Terrorism, and the Financing of Arms Proliferation (the New AML Law]

- **Cabinet Decision No. (10) of 2019** concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AML-CFT Decision") and its amendments.

- **Cabinet Decision No. (74) of 2020** Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments.

- **Cabinet Decision No. (58) of 2020** regulating the Beneficial Owner Procedures ("Cabinet Decision 58");

- **Guidance for Licensed Financial Institutions** on Digital Identification for Customer Due Diligence;

- **Cabinet Resolution No. (109) of 2023;** and

- **CBUAE/BSD Notice No. 1943.2022** Regarding AML/CFT Minimum Standards and Supervisory Expectations.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Role and Significance of CDD/KYC and Recordkeeping

What is CDD/KYC?

CDD/KYC is an ongoing, risk-based process to collect, assess, and record relevant information about customers and their related parties, business profile, and transactions, to appropriately assign and monitor the ML/TF/PF and other financial crimes risks exposure of the customer. CDD/KYC often happens before a new customer is onboarded, and then at regular intervals throughout a customer's relationship with the LFI. Specifically, LFIs should perform CDD/KYC in the following scenarios:

- **When establishing a business relationship:** Ahead of establishing a new customer-business relationship and conducting any transactions on a customer's behalf, LFIs should perform due diligence to verify the identity of the customer and its related parties, evaluate the customer's risk profile, understand the customer's business and expected transactions, and ensure the customer is not using a fake identity to access the LFI's products and services.

- **To analyse occasional transactions:** Certain transactions might require further CDD/KYC measures. For example, transactions over a material monetary amount will require an LFI to review and potentially update a customer's CDD/KYC information

- **When there is suspicious activity:** LFIs should implement additional CDD/KYC checks if the customer engages in unusual or potentially suspicious activity that requires further investigation, either due to the presence of a red flag or because the customer is engaging in activity that is inconsistent with their historical profile established at onboarding, or if the customer has been classified as a Related Party to a party of concern identified through transactional review, ownership and control, or public domain.

- **Unreliable identification:** If information a customer has provided is inaccurate, incomplete, or does not meet an LFI's internal requirements for CDD/KYC, LFIs should implement additional CDD/KYC measures to ensure that they can properly establish the identity of the customer and the nature and purpose of the customer's relationship with the LFI.

- **Periodic and trigger-event reviews:** LFIs should implement periodic CDD/KYC reviews for all existing customers with the review frequency corresponding to the risk profile of a customer, as well as one-off reviews due to a particular trigger event occurring related to the customer.

Core Elements of CDD/KYC

There are four core elements of a CDD/KYC program, each addressed in detail, later in this presentation:

Identifying a customer and verifying the customer's identity.

Identifying beneficial owner(s) and key senior personnel of a legal entity customer and verifying their identity using a reliable and independent source.

Understanding the nature, purpose, and transactional behavior of a customer relationship to develop a customer risk profile.

Ongoing monitoring of customer activity for reporting suspicious transactions and updating customer information and risk profile, as necessary.

Significance of CDD/KYC

- **Sophisticated Financial Crimes Threats:** Criminals use ever evolving means to engage in money laundering, terrorist financing, and proliferation financing by hiding behind complex corporate structures, forged documentation, and/or identity theft. Appropriately identifying and verifying customers, inter alia, understanding the nature of a customer's business, occupation or profession, source of income or SoW, SoF, expected activity helps LFIs protect their institution against financial crimes.

- **Interconnected Financial System:** The UAE's financial system is increasingly interconnected, and the harm done by illicit actors engaging in financial crime is global, impacting the financial integrity and stability of the international financial system**.** Appropriate CDD/KYC controls are crucial to an LFI building and maintaining trusting relationships with correspondent banks and other global financial institutions.

- **Non-Compliance Risks:** Regulatory, reputational, and financial consequences of non-compliance are all serious repercussions resulting from ineffective CDD/KYC controls. An LFI can suffer grave legal, reputational, and financial risk as a result of ineffective controls

Importance of Recordkeeping

Documentation: there should be sufficient documentation that allows an LFI to demonstrate:

- Why a specific customer was onboarded, with rationales increasing in granularity as customer risk rises;
- How the customer was risk rated; and
- What steps the LFI took to monitor the customer's activity to ensure it corresponded to the customer's risk profile throughout the relationship with the LFI.

Storage: data should be stored in a safe and reliable manner to support any internal processes, and allow easy access, when requested by regulators and law enforcement agencies, as authorized by UAE laws and regulations

Poor recordkeeping can lead to delays during audits and investigations**,** possibly resulting in missed deadlines for compliance reporting and increased scrutiny from regulators.

CUSTOMER DUE DILIGENCE

General CDD Principles

- CDD/KYC should not be treated as a “check-the-box” exercise. Staff should critically assess information provided by a customer, seek additional information or clarifications, if necessary, and raise identified issues to the appropriate Compliance officer.
- LFIs should develop and implement appropriate, risk-based, and sufficiently detailed procedures for collecting identification information, and conducting CDD/KYC at onboarding and on a periodic basis thereafter.
- LFIs also should develop policies and procedures that require the LFI to carry out CDD/KYC measures in special circumstances, e.g., carrying out occasional transactions in the form of wire transfers for certain monetary amounts.
- LFIs should prescribe situations where a customer should undergo Enhanced Due Diligence (“EDD”) or Simplified Due Diligence (“SDD”), as well as corresponding procedures for staff to follow.
- LFIs should not establish or maintain relationships with customers who are unable or unwilling to provide required CDD/KYC information, whether at onboarding or as a part of ongoing monitoring, periodic review, or event-driven review processes.

LFIs should develop and implement appropriate, risk-based, and sufficiently detailed procedures for collecting identifying information and conducting CDD/KYC both at onboarding and on a periodic basis thereafter. These procedures should address, at a minimum:

In addition to conducting CDD/KYC before or during onboarding and periodically thereafter, LFIs should undertake CDD measures in the following cases:

- Carrying out occasional transactions in favour of a customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked (i.e., a customer initiates several transactions to the same beneficiary or group of the same beneficiaries, which appear to be one transaction broken up into several smaller transactions);
- Carrying out occasional transactions in the form of wire transfers for amounts equal to or exceeding AED 3,500;
- Where there is suspicion of a crime; or
- Where there are doubts about the veracity or adequacy of previously obtained customer identification data

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Customer Identification and Verification (1/3)

Natural Persons

LFIs should verify an individual's identity using original documents, data, or information from a reliable and independent source. The following information should eb identified and verified:

- Full name;
- Permanent residential address;
- Date of birth;
- Place of birth:
- Name and address of employer;
- Intended purpose and nature of the relationship with the LFI; and
- Information that would determine PEP status

Legal Persons / Arrangements

LFIs should verify the following information of a legal person or arrangement's identity using original documents, data, or information from a reliable and independent sources:

- Name, legal form, and memorandum of association;
- Headquarters office address or the principal place of business;
- Articles of incorporation, bylaws or similar documents, attested by the competent authority within the UAE;
- Names of relevant key controllers or persons holding senior management positions with the legal person or legal arrangement;
- Information on ownership and structure of the legal entity;
- Intended purpose and nature of the relationship with the LFI; and
- Nature of the customer's business.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Customer Identification and Verification (2/3)

LFIs must identify and verify each customer's identity from a reliable and independent source, either using **documentary sources or non-documentary sources**:

Documentary Sources

For natural persons:

- Government-issued identification document, such as passport or national identification card;
- Residency may be confirmed with a utility bill, correspondence from a UAE government office, or official housing documentation like a mortgage or tenancy contract.

For legal persons / arrangements:

- Certificate of incorporation bearing an official government agency seal;
- Official extract from a government-maintained corporate registry; or
- An official government-issued corporate ID.

Non-Documentary Sources

For both natural and legal person customers:

- Scheduling a face-to-face customer meeting;
- Contacting a customer via phone, video conference, mail, or email to confirm they are still valid;
- Checking references with other financial institutions;
- Independent verification via public or private databases, corporate registries, or credit bureau; or
- Visiting the legal person customer's place of business, if practical.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Customer Identification and Verification (3/3)

Digital Identification and Verification

Article 8 of the AML-CFT Decision does not impose any restrictions on the form—physical or digital—that identity evidence should take, nor does it impose limitations as to the use of digital identification systems for the purpose of linking a customer's verified identity to a unique, real-life individual, provided this is done using a "reliable" and "independent" source.

Overall, LFIs should be aware of and utilize the following national-level identification systems and processes that exist or are under development in the UAE:

- **Emirates ID:** the mandatory identity card for all UAE citizens and residents issued by the Federal Authority for Identity, Citizenship, Customs and Ports Security ("ICP"). While issued as a physical card, the Emirates ID uses public key infrastructure to attach individual identities to digital certificates that can be used to sign and encrypt data, as well as fingerprint biometrics. LFIs should use the online Validation Gateway maintained by the ICP when verifying an Emirates ID card and should keep a copy of the card and evidence of its digital verification in accordance with its record-keeping policies.

- **UAE Pass:** the UAE's first national digital identity and signature solution that enable users –citizens, residents, and visitors in the UAE – to identify themselves to government service providers in all emirates through a smartphone-based authentication protocol and to sign documents digitally with a high level of security. The UAE Pass app uses biometric facial recognition software to verify and register users without requiring an in-person visit to a government services centre.

- **Emirates Facial Recognition:** an initiative launched by the UAE Ministry of Interior and ICP, together with private sector partners. The facial recognition initiative includes a "face fingerprint" system for digital verification of digital transactions and remote identities.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Beneficial Ownership Identification and Verification

The AML-CFT Law defines an ultimate beneficial owner (UBO) as a "natural person who owns or exercises effective ultimate control, **directly or indirectly**, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement, whether directly or through a chain of ownership, control or other indirect means. **The UBO of a legal person should be an individual or group of individuals.**
Another legal person cannot be classified as the UBO of a customer, no matter what percentage it owns. LFIs should continue tracing ownership all the way up the ownership chain until it identifies all individuals who own or control at least 25 percent of the LFI's customer.

Identifying UBOs of a Legal Person Customer

- The identities of all beneficial owners of a customer are all individuals who, individually or jointly, have a controlling ownership interest in the legal person of **25 percent or more.**
- If no individual meets this description (e.g., publicly listed entity), the LFI must identify and verify the identity of the individual(s) exercising control over the organization (e.g., CEO, CFO)

Identifying UBOs of a Legal Arrangement Customer

- The identity of the settlor, trustee(s), or anyone holding a similar position, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the arrangement.
- LFIs should also obtain sufficient information regarding the beneficial owner to enable verification of his/her identity at the time of payment or at the time he/she intends to exercise his/her legally acquired rights.

UBOs should generally be identified and verified *prior* to establishing a business relationship.

Establishing a Customer Risk Profile (1/4)

- LFIs should identify, assess, and, understand the ML/TF/PF and other financial crimes risks associated with its customers (i.e. customer risk assessment/rating) and should reflect this risk through assigning a customer risk rating.
- While there is no universal customer risk rating model that should be used across the financial sector, LFIs should consider the ongoing publication of information by the CBUAE and other UAE competent authorities to identify, assess, and understand the risks associated with their customers. General factors for LFIs to consider, at a minimum, when assessing customer risk profile include:

Products and services used by the customer;

Geographic locations, both of the customer and the counterparties they transact with; and

Type of the customer's business, customers, and counterparties.

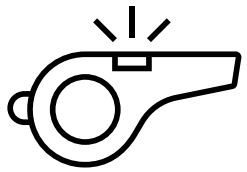
Each customer's ML/TF/PF risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behavior, and as such, appropriate due diligence should be applied in keeping with the specific situation and risk indicators identified.

Establishing a Customer Risk Profile (2/4)

There are several pieces of customer information an LFI should collect during the onboarding process to facilitate a comprehensive customer risk rating process.

Customer Information

- Nature of customer contact and state purpose of the account
- Source of funds / Source of wealth
- Customer occupation (for individual customers)
- Legal entity type and industry (for legal entity customers)
- Anticipated geography of a customer's expected activity
- Anticipated transaction volumes and values
- Anticipated products and services to be used throughout the relationship
- Anticipated channels for maintaining the relationship



To establish a proper customer risk profile, LFIs should understand the nature of the customer's business and the nature and purpose of the LFI's relationship with the customer, using the customer information above.

Obtaining sufficient understanding of the your customer allows the LFI to develop an activity profile for the customer, against which unusual or suspicious transactions may be identified.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Establishing a Customer Risk Profile (3/4)

Customer Segmentation

- The customer segmentation involves obtaining sufficient information to assign a customer to a customer segment.
- The process enables LFIs to appropriately divide customers into categories of risk and calibrating subsequent internal controls, such as applying EDD, setting up transaction monitoring thresholds, and identifying the customer's periodic review schedule.
- LFIs are encouraged to utilize a wide range of data elements collected as a part of baseline CDD/KYC when developing a customer risk rating and segmentation methodology.

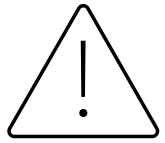
Customer information that enable an LFI to form a dynamic risk profile.

Source of Funds / Source of Wealth (SoF/SoW)

If an LFI determines that a particular customer represents a higher-risk relationship and warrants EDD, the LFI should use reasonable means to collect information regarding the customer's SoF or SoW.

- **Identifying the SoF**: means identifying the direct source of the funds that are used to initially fund a customer's account, and any funds that are transacted through the account during the course of the business relationship (such as the customer's salary or the sale of a real estate property).

- **Identifying the SoW:** means identifying the sources that have generated or significantly contributed to the customer's total net worth (such as a customer's inheritance). Where the size of balances in the account is inconsistent with a customer's stated SoW and/or where the initial source of capital for an account is unclear, LFIs should take additional steps to corroborate SoW.
- LFIs should verify the SoF/SoW by obtaining evidence from the customer.



LFIs should critically assess the SoF/SoW of a customer, particularly in the highest-risk relationships. LFI training should include examples of red flags staff should be aware of when assessing SoF/SoW.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Establishing a Customer Risk Profile (4/4)

Expected Activity

- Collecting information regarding a customer's expected account activity and assessing self-reported expected activity is required for LFIs in order to determine the reasonableness of certain transactions.
- Where the customer's activities are inconsistent with customer's stated purpose of the account and the transactional activity profile, the LFIs should conduct additional transaction analysis and collect sufficient information, such as a written explanation from the customer, supporting business documentation, or past financial statements, to understand and corroborate the self-reported activity.

Geographic Information

- Geographic component represents an important part of the overall customer risk rating and assessment and should be used when developing a customer risk rating methodology.
- It is crucial for the LFI to collect and assess the geographies/jurisdictions where a customer resides and expects to transact or do business.
- Assessing whether any reported jurisdictions are those with weak regulatory AML/CFT frameworks, subject to UN or UAE sanctions, or where FATF has called for increased monitoring (i.e., gray list) is a key factor in a customer risk rating process.

Prohibited Customers

- LFIs should have a customer acceptance policy (risk appetite) that outlines the types of customers the LFI will not accept as a matter of policy due to unacceptable legal, regulatory, or reputational risks they pose to the LFI.
- Customer information collected allows employees to appropriately identify such types of customers and prevent them from onboarding or continuing an existing relationship.

Ongoing Monitoring

Ongoing Monitoring

- All customers should be subject to ongoing monitoring throughout the business relationship, as an element of both continuous CDD/KYC and suspicious activity reporting.
- Depending on the nature, size and complexity of the business, LFIs can use automated, manual or a combination of both, monitoring systems and processes to conduct ongoing monitoring. Bigger LFIs are recommended to use automated transaction monitoring systems.

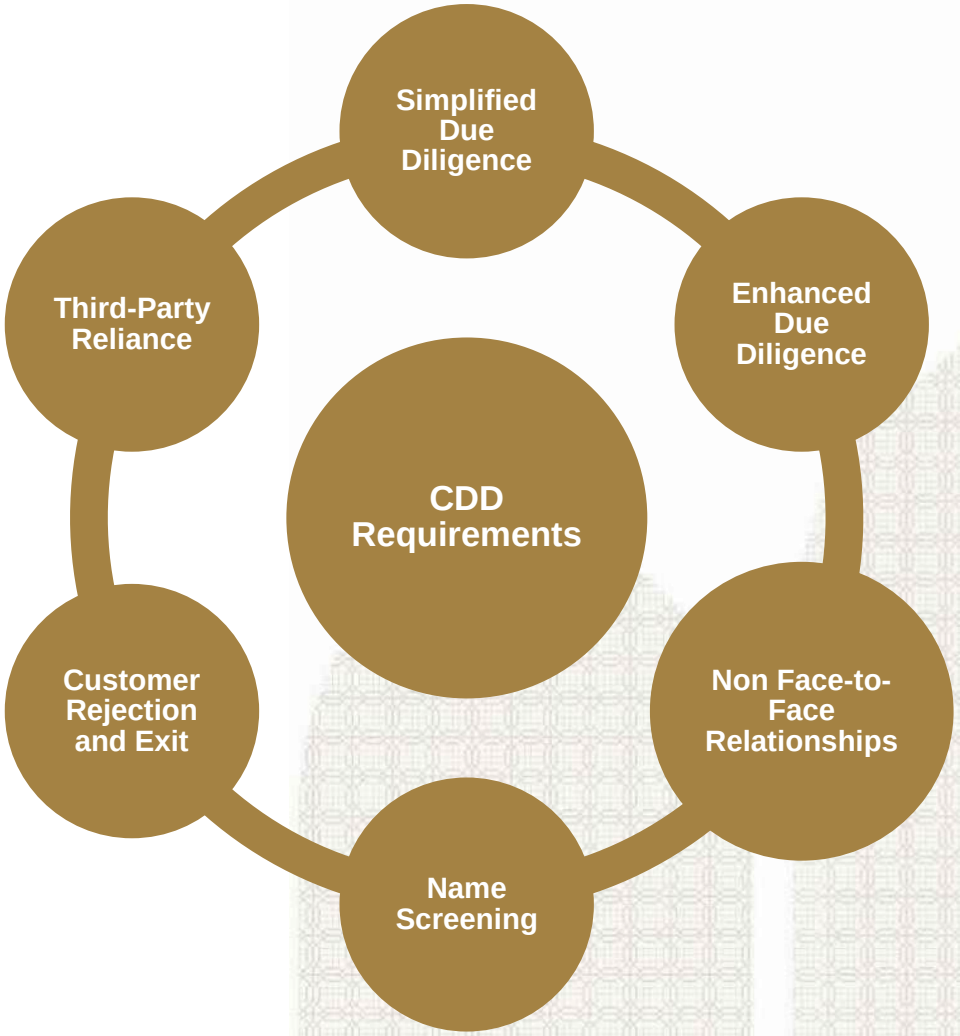
Periodic and Event-Driven Reviews

- LFIs should develop standards and procedures outlining the frequency and process of periodic customer reviews, driven by the assigned customer risk rating. For example, a high-risk customer profile may be reviewed annually, while a low-risk profile reviewed every three years.
- Event-driven reviews stem from the occurrence of a material change to a customer's profile, e.g., a change in customer legal name, unexplained changes in account activity, or changes in legal entity ownership.

Risk Profile in Transaction Monitoring

- CDD/KYC establishes a customer's risk profile and expected activity against which an LFI can review a customer's actual activity to assess potential variances.
- In line with the risk-based approach, LFIs should use a customer's risk profile to inform the degree and nature of transaction monitoring that the LFI applies to its customers. For customers identified as high risk, LFIs may choose to conduct enhanced transaction monitoring.
- Transaction monitoring feeds into the LFI's suspicious activity reporting program and wider AML/CFT compliance program by flagging high-risk and potentially suspicious transactions and typologies.

Additional CDD Requirements



Simplified Due Diligence for Lower-Risk Scenarios

As per Article 4.3 of the AML-CFT Decision, an LFI may perform simplified due diligence (SDD) measures in relation to a customer, a beneficial owner of a customer, a natural person appointed to act on behalf of a customer, or a beneficiary or other payee if it is satisfied that the risks of ML/TF/PF are low. In all cases, the LFI must document the details of its analysis that led to its comfort conducting SDD.

Examples of potentially lower-risk scenarios – where no other countervailing risk factors are present:

- The customer is a UAE government entity, including UAE state-owned enterprises;
- The customer is an entity listed on a stock exchange and subject to regulatory disclosure requirements that identify a customer's UBOs; and
- The customer is rated as low risk under the LFI's documented customer risk rating methodology. The LFI's customer risk rating methodology should meet the minimum requirements as provided for in section 6.1.1 (Assessing Customer and Business Relationship Risk) of the CB Notice No. 3599 of 2023.

Of note, an LFI should *not* perform SDD measures where:

- A customer or any UBO of the customer is from or in a country or jurisdiction identified as non-cooperative by the FATF;
- A customer or any UBO of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the LFI, or as notified by local regulatory or supervisory authorities; or
- The LFI suspects that ML, TF, PF, or other criminal activity is involved.

Enhanced Due Diligence for Higher-Risk Scenarios

The AML-CFT Law and the AML-CFT Decision EDD obligations on LFIs with respect to the following classes of customers or transactions:

- Customers that are foreign or domestic PEPs with high-risk factors, which include the direct family members or associates known to be close to the PEPs (Article 15 of the AML-CFT Decision). Ruling family members classified as domestic PEPs should not have a SoW/SoF verification requirement, if the information can be verified through publicly available and reliable sources; and
- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries (Article 15 of the AML-CFT Decision).

Examples of Higher-Risk Scenarios

- The customer belongs to a higher-risk industry (e.g., financial services;
- The ownership structure of a legal entity customer appears unusual or unnecessarily complex;
- The customer is a cash-intensive business; and
- The legal entity customer is a personal asset-holding vehicle.

Examples of EDD Measures

- Obtaining approval from the LFI's senior management to establish or continue a business relationship with the customer;
- Commissioning external intelligence reports when it is not possible for the LFI to obtain information via public sources; and
- Requiring the first payment to be carried out through an account in the customer's name with an LFI subject to similar CDD/KYC standards.

Non-Face-to-Face Relationships

Heightened ML/TF/PF risks may arise from establishing business relationships or undertaking transactions according to instructions conveyed by customers over the internet (absent personal contact via video teleconference), digital application, post, fax, or telephone. An LFI should note that online applications and transactions may pose greater risks than other non-face-to-face due to several factors.

The measures taken by an LFI for verifying the identity of customers and UBOs in the context of non-face-to-face relationships will depend on the nature and characteristics of the product or service provided and the customer's risk profile. LFIs should apply additional checks to mitigate the risks of performing identity verification without face-to-face contact, such as:

- Telephone contact with the customer at a residential or business number that can be verified independently;
- Confirmation of the customer's address through an exchange of correspondence or other appropriate method; and
- Subject to the customer's consent, telephone confirmation of the customer's employment status with his or her employer's human resource department at a listed business number of the employer;

LFIs are reminded to continue to explore digital identification systems that can enable remote customer identification and verification, support remote financial transactions, and otherwise facilitate non-face-to-face business relationships and transactions

Name Screening

LFIs should screen the following parties against relevant ML/TF/PF information sources (such as negative media databases), databases of known PEPs, and internal watchlists (such as lists of customers previously exited or denied onboarding for financial crime reasons) prior to a customer's onboarding and keep records of true matches as part of the KYC documentation:

All customers, regardless of risk rating or risk profile;

- UBOs of legal entity customers;
- Natural persons appointed to act on behalf of the customer;
- Names of relevant persons holding senior management positions with the legal person (such as directors, partners, authorized signatories, and senior executives); and
- Natural persons having executive authority over customers that are legal arrangements.

Importantly, the parties listed above should be screened against the UNSC and UAE Local List prior to onboarding and on an ongoing basis thereafter. The results of screening and assessment by the LFI should be documented.

Customer Rejection and Exit

Under Article 14.2 of the AML-CFT Decision, LFIs should not deal with any person on an anonymous basis or any person using a fictitious name and using pseudonyms, fictitious names, or numbered accounts without the account holder's name.

If an LFI is unable to undertake the CDD/KYC measures, or identifies a confirmed match to a party included on applicable Sanctions Lists, the LFI should:

- Not onboard the customer;
- In case of a confirmed match, freeze without delay and without giving a notice to the customer, funds owned or controlled, wholly or jointly, directly or indirectly, by a sanctioned person or by a person or organization acting on behalf of or at the direction of a sanctioned person;
- Exit the relationship if one has been established;
- For insurance operators, not make any payment to a payee or beneficiary under the customer's policy or other insurance relationship; and
- Maintain all related records

In case of a confirmed match, the LFI should freeze without delay and without giving a notice to the customer, funds owned or controlled, wholly or jointly, directly or indirectly, by a sanctioned person or by a person or organization acting on behalf of or at the direction of a sanctioned person, and notify EOCN within five business days.

Third-Party Reliance

Third-party reliance enables an LFI to rely on the CDD measures carried out by another vendor. However, it is important to remind LFIs that the Compliance Officer of the LFI bears the ultimate responsibility to verify and validate CDD information provided by the third-party.

Therefore, third-party reliance in no way relieves the relying LFI of performing other CDD measures, including understanding a customer's expected activity, determining whether customers are high-risk, and assessing whether a customer's transactions constitute suspicious activity.

LFIs are permitted to rely on certain third parties to perform the following elements of CDD measures:

- Identifying a customer and verifying a customer's identity using reliable, independent source documents, data, or information;
- Identifying a beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that an LFI is satisfied that it knows the identity of the beneficial owner.
- Understanding and obtaining information on the purpose and intended nature of the business relationship.

Third-Party Reliance

LFIs are permitted to rely on certain third parties – financial institutions or designated non-financial businesses and professions ("DNFBPs") – to perform the following elements of CDD measures:
a) Identifying a customer and verifying a customer's identity.
b) Identifying a beneficial owner and taking reasonable measures to verify the identity of the beneficial.
c) Understanding and obtaining information on the purpose and intended nature of the business relationship.

When entering into a third-party reliance arrangement, LFIs should ensure the third party has appropriate measures in place to comply with the UAE's AML/CFT regulatory requirements. LFIs should ensure that the following criteria are met:

- immediately obtain the necessary information concerning elements (a) to (c) as outlined above,
- take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- satisfy itself that the third party is regulated, supervised or monitored for ML/TF/PF compliance, and adheres to the CDD and record-keeping requirements outlined in the AML-CFT Decision.
- When determining in which countries the third party that meets the conditions can be based, LFI should have regard to information available on the level of country risk.

The third-party reliance does not apply in the context of outsourcing, service provider, or agency relationship. The third-party reliance is only acceptable in the case of reliance on other financial institutions or DNFBPs conducting CDD, which typically means that the third party will have an existing business

Record keeping

Record keeping (1/2)

LFIs should maintain detailed records associated with their ML/TF/PF risk assessment and mitigation measures as well as records, documents, data, and statistics for all financial transactions, all records obtained through CDD/KYC measures, ongoing monitoring, sanctions screening, account files and business correspondence, copies of personal identification documents, and STR or SAR files and results of any analysis performed.

The statutory retention period for all records is at **least five years** from the latest date of the following trigger circumstances:

- from the date of completion of the transaction;
- termination of the business relationship with the customer;
- completion of the inspection by the CBUAE;
- issuance of a final judgment of the competent judicial authorities; or
- liquidation, dissolution, or other form of termination of a legal person or arrangement.

Internal procedures should clearly show how the LFI store records – whether physical or digital form , or both; whether originals or scanned/electronic copies.

Record keeping (2/2)

An LFI should maintain the following types of records as part of a well-documented AML/CFT compliance program:

- Policies, procedures, and controls
- Documentation on third-party reliance
- Customer information
- Transactions
- Customer screening
- External and internal compliance reports
- Other customer due diligence records
- Investigation records
- Information that is not processed
- Regulatory requests and remediation
- Training Monitoring

Conclusion and Questions

Thank You