ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

Financial Crime Prevention Unit
Financial Services Regulatory Authority
ADGM Authorities Building,
ADGM Square,
Al Maryah Island,
Abu Dhabi

27 April 2021

Notice No.: FSRA/FCPU/09/2021

To: Senior Executive Officers (SEO), Money Laundering Reporting Officers (MLRO) and Principal Representatives (PR) of Approved Persons

Dear SEO/MLRO/RP,

RE: Know Your Customer (KYC) Guidelines for Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs)

The Financial Crime Prevention Unit has issued a guidance concerning KYC. The guidance has been published on the FCPU website and can be accessed **here.**

The main purpose of the guidance is to provide clarity to Relevant Persons and to assist them in understanding their obligations under the UAE 'Anti-Money Laundering and Combating the Financing of Terrorism' (AML/CFT) framework, as well as the requirements contained in the Financial Services Regulatory Authority's (FSRA) AML and Sanctions Rules and Guidance. These laws and regulations set out the minimum standards that must be adhered by FIs and DNFBPs in the creation and implementation of their KYC policies, processes and procedures.

Relevant Persons should pay close attention to the key points highlighted in this guidance and apply them in a risk-based and proportionate manner that reflects the nature, size and complexity of their business operations.

Annex: KYC guidance document

Sincerely,

Financial Crime Prevention Unit

ADGM

Know Your Customer (KYC)

Guidelines for Financial Institutions (FIs)
& Designated Non-Financial Businesses & Professions (DNFBPs)

Contents

1. Introduction

The purpose of these guidelines is to provide assistance to Relevant Persons, in order to assist them in understanding their obligations under the United Arab Emirates' (UAE) 'Anti-Money Laundering and Combating the Financing of Terrorism' (AML/CFT) framework[1], as well as the requirements contained in the Financial Services Regulatory Authority's (FSRA) AML and Sanctions Rules and Guidance. These laws, regulations and rules set out the minimum standards that must be adhered by FIs and DNFBPs in the creation and implementation of their KYC policies, processes and procedures.

Relevant Persons should pay close attention to the key points highlighted in this paper and apply them in a risk-based and proportionate manner, considering the size, nature, and complexity of their business operations.

These guidelines are not intended to be read in isolation from other UAE or ADGM relevant legislation or developments in international policy and best practice and, to the extent applicable, Relevant Persons need to be aware of, and take into account, how these aforementioned matters may affect the Relevant Person's day-to-day operations.

The terms and abbreviations used in these guidelines should be interpreted with reference to the definitions set out in the FSRA AML and Sanctions Rules and Guidance, which can be accessed through the following link:

https://www.adgm.com/operating-in-adgm/financial-crime-prevention/aml.

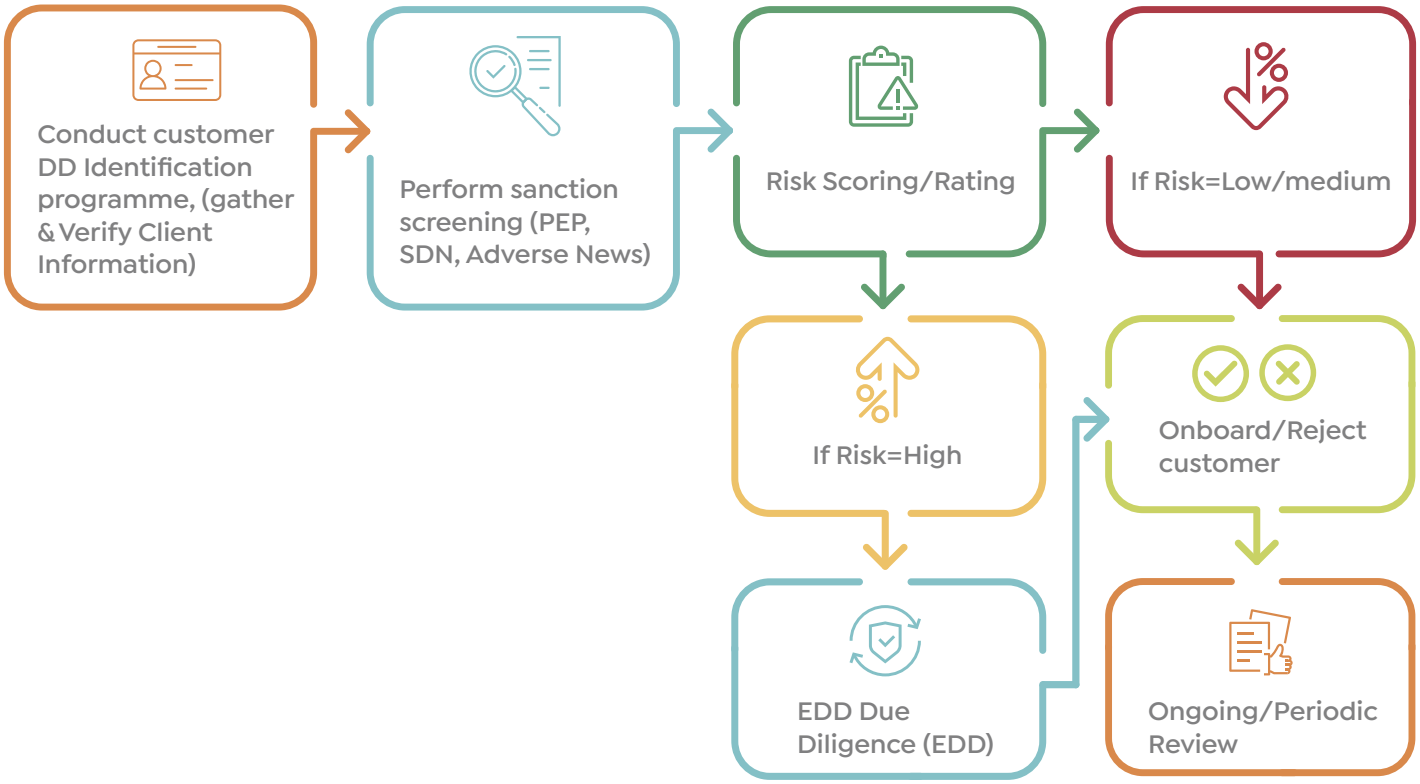
[1]The UAE's AML/CFT legal framework is unified under the following laws:

- Federal Law No. 20 of 2018, on "AML/CFT and the Financing of Illegal Organizations"
- Cabinet Resolution No. 10 of 2019, "Concerning the Executive Regulation of Federal Law No. 20 of 2018 on AML/CFT and Financing of Illegal Organizations"
- Cabinet Resolution No. 20 for 2019 concerning "the UAE list of terrorists and implementation of UN Security Council decisions relating to preventing and combating financing terrorism and leveraging non-proliferation of weapons of mass destruction, and the relevant resolutions"- superceded by CR 74 of 2020

2. General KYC Compliance Guidelines

2.1. Customer On-Boarding

2.1.1 A Relevant Person shall verify the identity of the customer and beneficial owners before or during the course of establishing a business relationship or opening an account; or before carrying out a transaction for a customer with whom the Relevant Person is not in an established business relationship.



2.1.2 Relevant Persons must consider the following factors to assign the appropriate risk rating to their customer: For example, if a customer is rated as "High" then all the below factors should be considered, whereas if the customer is rated as "Low" or "Medium" Relevant Persons should take into consideration the factor indicated by (*) in the below diagram.

2.1.3 Relevant Persons should assign a customer with either a low, medium or a high-risk rating or use a numerical sliding scale, such as 1 to 100 with at least three differentiated risk ratings (as per guidance note 1, AML rule 7.1.3). It is important that the risk rating methodology is documented in the Relevant Persons AML policy.

2.1.4 Relevant Persons must also obtain an understanding of the intended purpose and nature of the business relationship, as well as, in the case of legal persons or arrangements, of the nature of the customer's business and its ownership and control structure.

2.1.5 Ongoing AML reviews do not end after on-boarding a customer. Depending on the risk classification of the customer or based on trigger events, there must be ongoing reviews of the customer's transactional activities that are commensurate with their risk classification. The profiles of high-risk customers should be reviewed at least once annually or as appropriate.

2.1.6 To meet this requirement, Relevant Persons are required to design and implement ongoing monitoring frameworks. They may need to segment their customer groups and establish appropriate parameters and risk scenarios to better detect deviations of customers' activities from their stated purpose of business and expected transactions or behaviours.

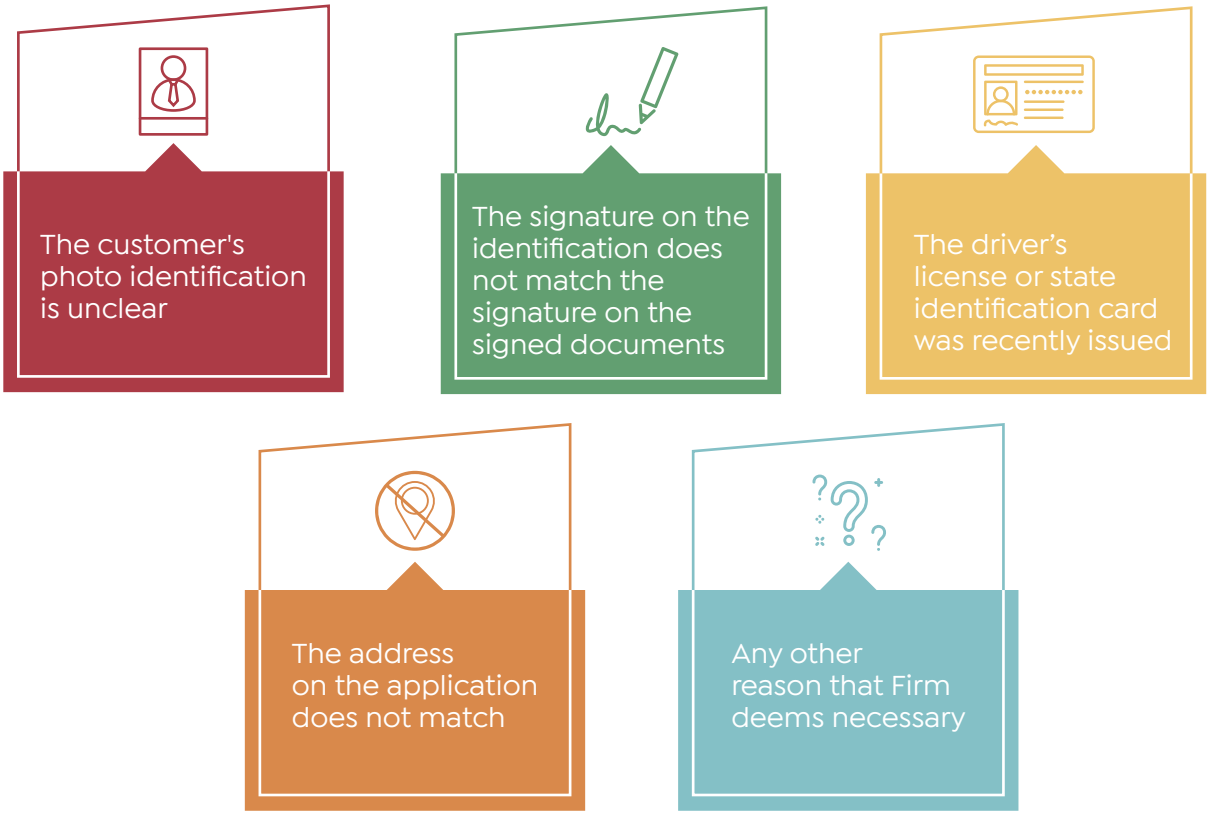
2.1.7 Relevant Persons must carry out regular training and awareness proportionate to the AML risks of the business and the Employee role.

2.2 Customer Due Diligence

2.2.1 In order to fulfil the above obligations, Relevant Persons are obliged to undertake customer due diligence (CDD) measures (including verifying the identity of customers, beneficial owners, beneficiaries, and Controlling Persons). The information and the evidence obtained from a customer[2] should be accurate, clear, and valid at the time of verification. In addition, Relevant Persons are required to take appropriate steps to identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks in relation to their customers.

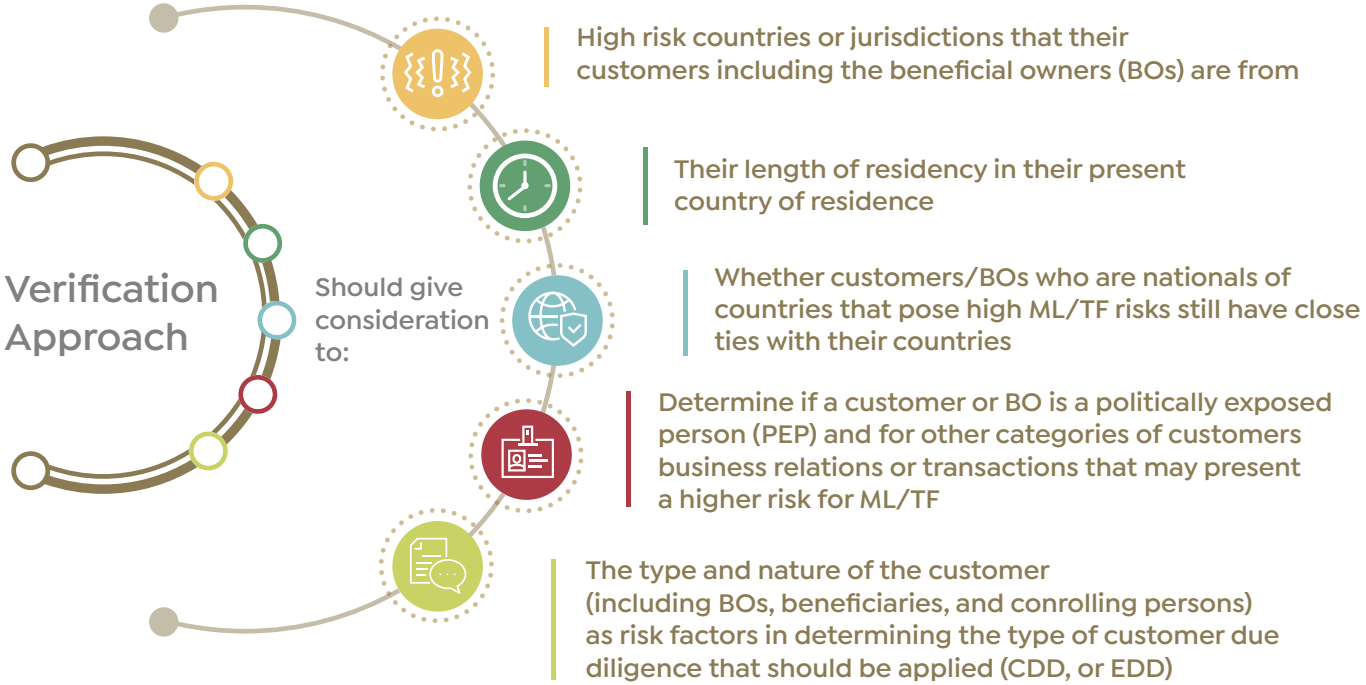
2.2.2 Relevant Persons must carry out **periodic reviews** to ensure the adequacy of the CDD information about its customers and their beneficial owners. Relevant Persons should maintain recent passport copies, identify documents to corroborate residential and/or business addresses and ensure that share registers are accurate and up to date. Where applicable, Relevant Persons should adjust the risk rating assigned to customers in light of any new money laundering risks.

2.2.3 The Firm should require additional identification if:



[2]The types of information and the evidence that should be obtained for each type of customers are highlighted under the AML Rules and Cabinet Resolution No.10 2019, and AML/CFT guidelines for FIs and DNFBPs

2.2.4 In addition, as a part of verification, Relevant Persons must give due consideration to the below highlighted elements to avoid the misclassification of a customer or beneficial owner with potentially high ML/TF risk as low risk, and vice versa, solely based on their country of residence.



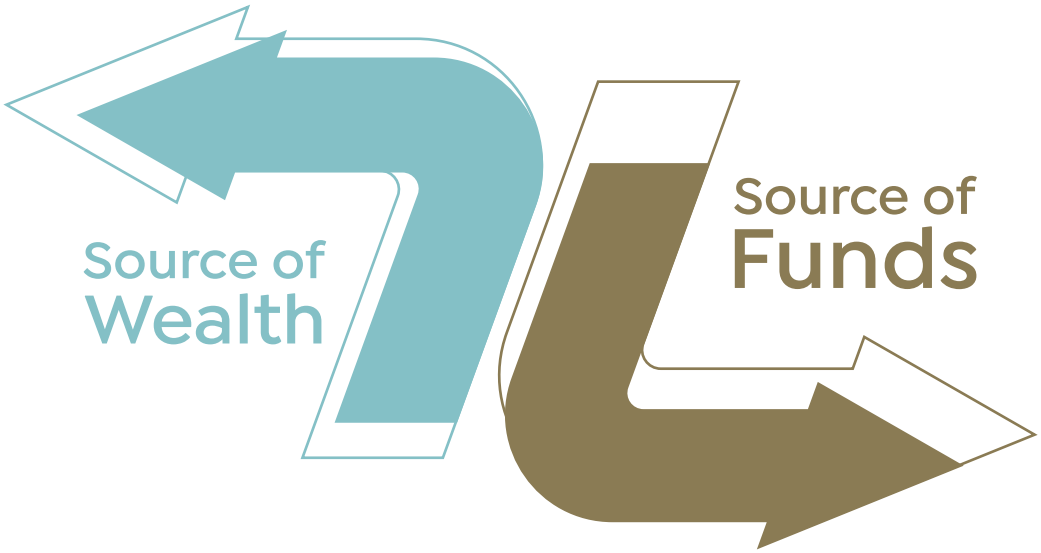
2.2.5 Relevant Persons must consider the type and nature of the customer (including beneficial owners, beneficiaries and controlling persons) as risk factors in defining the type of due diligence that should be applied, (i.e. determining whether routine CDD, or enhanced CDD is warranted). Relevant Persons are also obliged to put in place appropriate risk management systems to determine whether a customer, beneficial owner, beneficiary or controlling person is a PEP.

Noting that regardless of the type of CDD, the core components of a customer's identification generally remain the same in all cases:

Personal Data	Full name
	Identification number
	Nationality
	Date and place of birth (or date and place of establishment, in the case of a legal person or arrangement)
Principal Address	The current residential address of a natural person, or
	The registered address of a legal person or arrangement

2.2.6 Relevant Persons must undertake appropriate CDD that is commensurate with the money laundering risks the customer presents. Enhanced CDD measures must be assigned to customers with a high-risk[3] rating or if the beneficial owners are PEPs. This approach requires additional measures to be conducted on a case-by-case basis. On the other hand, for customers assigned a low-risk rating, the requirements may be modified according to the assessed risk. (Refer to Cabinet resolution No. 10 of 2019 and AML rules 8.3.2, 8.4.1 and 8.5.1).

2.2.7 As a result, Relevant Persons must perform sufficient enhanced CDD measures for high-risk customers[4] by obtaining a proper understanding of the separate requirements related to source of wealth (SOW) and source of funds (SOF), which are elaborated in the FSRA AML Rules. Corroboration of customers' representations using independent sources of information is important for high-risk customers in order to detect customers whose funds may be of illicit origin.



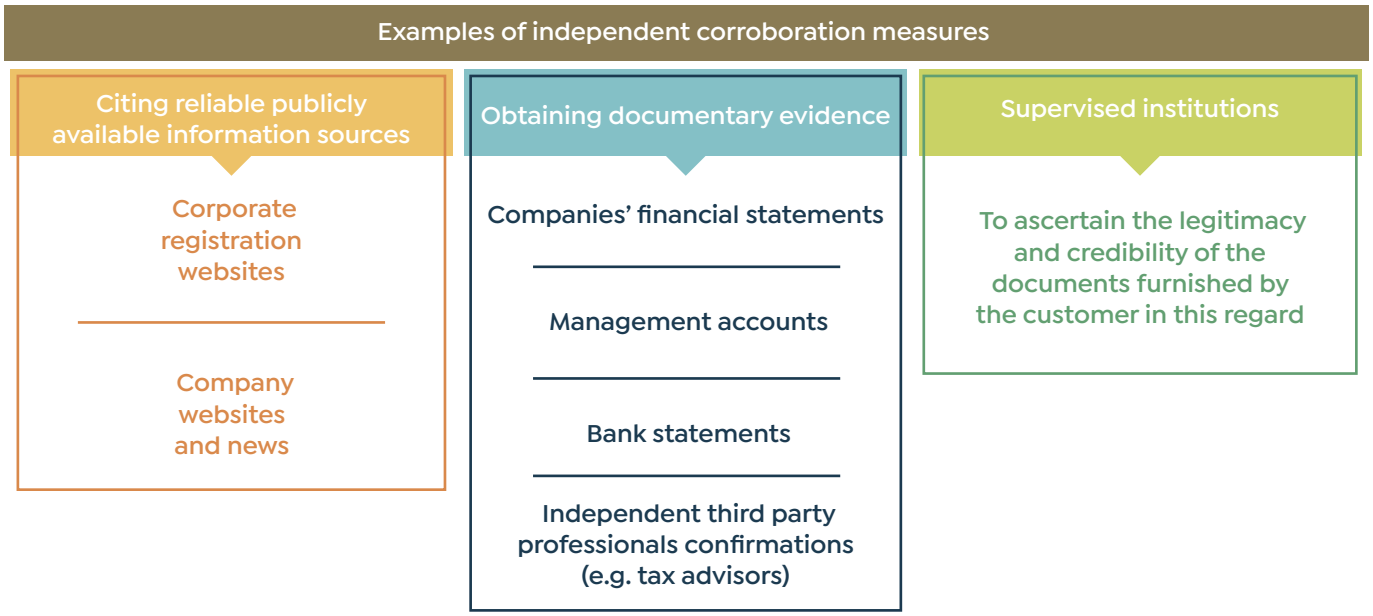
Note:

"In the circumstances when Relevant Persons are called to conduct occasional transactions or non-recurring transactions on an amount equal to or more than USD15,000 for customers that they do not hold accounts for, Relevant Persons must identify and verify the customer's identity including any beneficiaries or controlling persons. Relevant Persons should also apply proportionate risk-based measures that could include, but is not limited to, obtaining an understanding of the nature of the customer's business and the purpose of the transaction in question. Where there are doubts over the truthfulness or accuracy of such information, Relevant Persons should consider raising a Suspicious Activity Report."

[3]The AML/CFT guidance defines a high-risk customer as a customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by FIs, or DNFBPs or the Supervisory Authority.

[4]The AML Rules 7.1.2 and the AML/CFT guidelines highlighted the requirements for a high-risk customer

2.2.8 In addition, Relevant Persons should also assess and validate the plausibility and reasonableness of a customer's net worth against their understanding of the customer's background by obtaining supporting documentation and/or using public sources of information as reference points.



2.2.9 After performing enhanced CDD, Relevant Persons must obtain the approval of senior management to establish or continue business relations with high risk customers or where the beneficial owner is a PEP, or for other categories of customers that present a higher risk for ML/TF purposes. Approval by senior management is also needed if a customer subsequently becomes a PEP or presents a higher risk for ML/TF due to a change in circumstances.

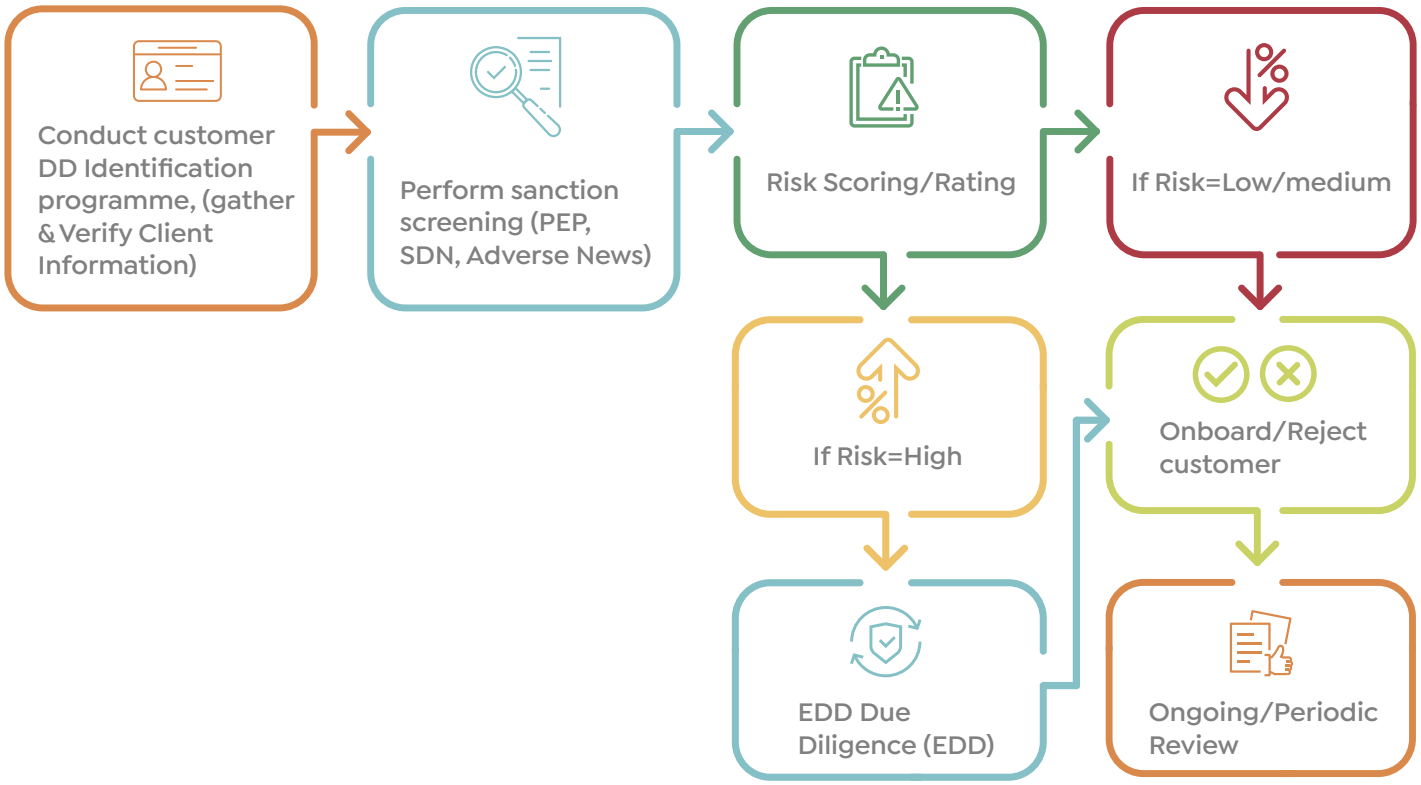
2.2.10 Only after due diligence has been carried out should a customer be on-boarded in accordance with company policies,procedures and requirements. Customer on-boarding is the final phase in the KYC on-boarding lifecycle - although CDD must continue throughout the time there is a relationship with the customer. In the event that the application poses an unacceptable risk, then the next step in the process is for the MLRO or compliance officer to reject the application and record the findings of the due diligence review.

2.2.11 Whenever Relevant Persons have a suspicion of money laundering and they reasonably believe that performing due diligence may tip-off the customer, they may opt not to carry out due diligence measures and instead submit a Suspicious Activity Report to the Financial Intelligence Unit (FIU) through the "goAML" platform stating the reasons as to why due diligence was not conducted.

2.2.12 In order to fulfil this obligation, Relevant Persons have to ensure that they have in place a robust process for investigating, reporting and documenting suspicious activities to the FIU. To fulfil these requirements, Relevant Persons must submit a request to obtain access to the designated secure electronic reporting platform, "goAML".

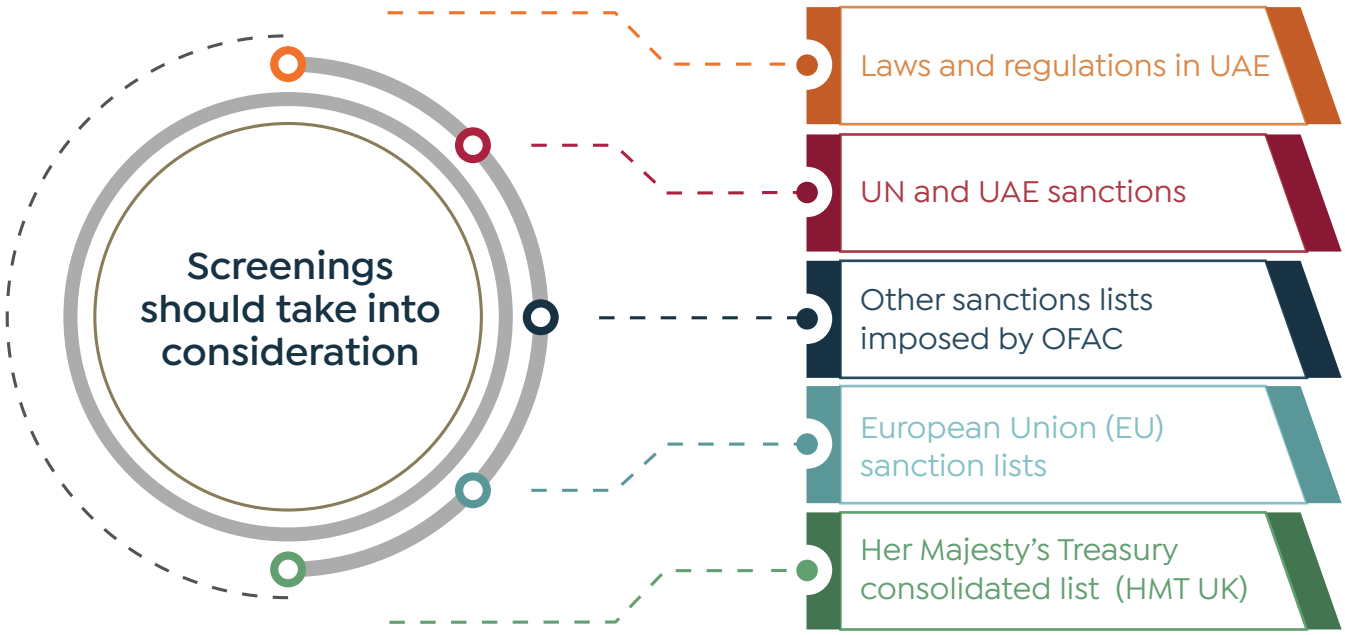
2.3. Screening Processes

2.3.1 Relevant Persons should implement an automated AML/CFT **screening process** to help detect PEPs, customers and transactions with high ML/TF risks. A screening framework and processes should be in place, both at the point of on-boarding and on an ongoing basis, to ensure that customers, business relations and transactions with high ML/TF risks are appropriately identified in a timely manner and are subjected to enhanced CDD measures where the findings warrant further verification.



2.3.2 The AML/CFT screening process should also incorporate thorough background searches into their due diligence procedures using tools such as:

2.3.3 Relevant Persons must perform regular screening processes of their existing customer base. The ongoing screening process allows Relevant Persons to promptly identify customers who are, or subsequently have become, PEPs or people with high ML/TF risks. The screening should take into consideration any of the below specified lists in conjunction with the requirements under the UAE laws and regulations:



2.3.4 Moreover, the names of on-boarded individuals and organizations that were not subject to sanctions, watch-lists or blacklists at the time of on-boarding should still subject to ongoing screening on a daily basis.

2.4. Reliance on a Third Party

2.4.1 Relevant Persons that rely on third parties must undertake due diligence to ensure the fitness and propriety of such parties. They must also implement adequate measures to ensure the third party's adherence to the requirements of the FSRA AML Rules and UAE AML/CFT Laws in relation to CDD are upheld.

2.4.2 Relevant Persons must be aware that where there is reliance on third parties in the CDD process, such as when an entire function is outsourced or when reliance is placed on the use of software and/or technology, they remain responsible for their AML/CFT obligations.

2.4.3 Relevant Persons are required to take responsibility for conducting ongoing monitoring of their business relations with customers and cannot rely on third parties to do so. Noting that for customers who present higher risks, Relevant Persons should endeavour to apply a higher standard to better assess, monitor and mitigate the ML/TF risks posed. Furthermore, they must secure the necessary information and documentation and retain them for the requisite period determined by the Regulator. In the event where third parties possess ultimate control of customer and transactional information, they should enter into agreements allowing them with unfettered and timely access to customer and transaction records. In addition to maintaining high standards on data security and storage, Relevant Persons must address any data protection and legal implications where CDD information is maintained by a third party provider.

3. Conclusion

For ADGM to remain as a trusted financial centre, it is important that Relevant Persons maintain effective AML/CFT controls to prevent the abuse of their products and services for illicit purposes. Amidst evolving ML/TF typologies, robust KYC is essential for Relevant Persons who are required to continually review, adapt and enhance their AML/CFT controls in order to remain effective. Relevant Persons are further encouraged to consider the use of new technology for tools and techniques and data analytics to improve their KYC on-boarding process.

Overall, Relevant Persons may also consider conducting a gap analysis in light of this guidance paper. ADGM will continue to provide guidance and share sound practices to improve industry practices.