UNITED ARAB EMIRATES
MINISTRY OF ECONOMY

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

Implementation Guide For

DNFBPs on

CUSTOMER RISK-ASSESSMENT (CRA)

November, 2024
Version 0.3.1.1

Customer Risk-Assessment (CRA)

Introduction:

DNFBPs are required to identify, assess, and understand their risks in concert with their business nature and size, and comply with the following: (a) Considering all the relevant risk factors such as clients, countries or geographic areas; and products, services, transactions and delivery channels, before determining the level of overall risk and the appropriate level of mitigation to be applied. (b) Documenting risk assessment operations, keeping them up to date on on-going basis and making them available upon request[1].

The ultimate purpose for conducting a customer risk assessment is to develop your understanding of the ML/TF and PF risks generated by DNFBPs clients, so that, when interacting with higher-risk clients, you can more effectively allocate your resources and implement more robust controls to mitigate the risks associated.

This document is limited to customer risk assessment and needs to be read in conjunction with the AML/CFT Law, by-law, and the MOE's AML/CFT Guidelines for Designated Non-Financial Businesses and Professions.

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

Customer Risk Assessment vs. Institutional Risk Assessment:

The customer risk assessment focuses on evaluating the risk that individual or corporate clients present in relation to ML/TF/PF. The CRA's include identifying high-risk clients, adjusting monitoring and due diligence procedures accordingly, and mitigating specific risks associated with them. This involves analyzing customer characteristics, behaviors, transaction patterns, and geographic risks to assess the likelihood of involvement in financial crimes. This assessment helps determine the appropriate level of due diligence and monitoring required, especially during customer onboarding and periodic reviews.

On the other hand, the Institutional Risk Assessment (IRA), focuses on assessing the institution's overall risk of exposure to ML/TF/PF (not the individual risks) by taking into consideration a wide range of internal and external factors that may impact the institution's

[1] Article 4, Section 2, 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.

overall performance and stability such as, industry-specific risks, operational processes, internal policies, regulatory Compliance, and the effectiveness of existing AML/CFT policies and procedures. It aims to ensure that the organization can successfully prevent, detect, and respond to threats of money laundering and terrorist funding, the institutional risk assessment seeks to identify and reduce risks at the institutional level.

Both CRA and IRA are essential components of an organization's comprehensive risk management framework, but they serve different purposes. While CRA is focused on the customer level, IRA addresses risks at the institutional level. It is important for organizations to regularly conduct both assessments and align them with national risk assessments and sector-specific requirements to ensure an integrated approach to risk management.

This guidance will focus on the customer risk assessment (CRA), for more information about the institutional risk assessment, please refer to the comprehensive Guidance for the DNFBPs[2].

What is CRA:

A CRA is a risk-based assessment that DNFBPs need to undertake for their clients (or prospective clients). This risk assessment must, at minimum, factor in the type of customer (individual or corporate) prior to moving forward through the next steps of your organization's due diligence processes, jurisdiction of the customer, purpose and intended nature of the customer's business, the beneficial ownership transparency (the complexity of the legal structure and controls of the ownership of the customer), the product and/or service offered, and the delivery channel. The result of the CRA determines the customer's risk rating.

The outcome of the CRA, which could be descriptive (i.e., High, Medium and Low) or numerical (i.e., 1 to 10), will determine the level of Customer Due Diligence (CDD) to be performed and the frequency of reviews to be undertaken in relation to that customer. For example, where a customer poses higher risk and is rated high risk from ML/TF perspective, it will be required to conduct Enhanced Customer Due Diligence (Enhanced CDD).

Sample process flow:

Apply CRA → Apply suitable controls and mitigation measures → Business relationship/transactions

[2] https://www.moec.gov.ae/en/aml

What is a High Risk Customer?

The customer who constitutes a risk whether due to his own personality, activity, business relationship, business nature, or the geographical territory, including for example customers from high-risk countries, non-residents who do not have an identification card from the state, personalities with complex structures or who perform complex operations or operations lacking obvious economic or legal objectives, persons who perform intense cash transactions, enter into transactions with anonymous third-persons, or carry out non face-to-face transactions or any other high-risk transactions defined by financial institutions, DNFBPs, or the regulatory bodies. [3]

Why CRA is important:

The main purpose of the assessment is to identify the ML/TF/ PF risks to which a firm may be exposed from each client/transaction, either in the course of a business relationship, or for an occasional transaction. The more complex this interaction is, the more rigorous a customer risk assessment needs to be.

By assessing the risk associated with clients, DNFBPs can determine the level of procedures to be performed and the controls to be applied to manage risk effectively. For example, enhanced due diligence measures are applied to manage the increased risk for clients categorized as posing a high risk to the business.

When it is required to apply the CRA?

- Onboarding New Customers: Prior to establishing a business relationship with a customer, and at regular intervals throughout the business relationship, depending on the risk rating of your customer.
- Periodic Reviews: Whenever there is a change in the customer's circumstances or the nature of the business relationship. For example, change in ownership, nature of the products or services being offered, or transaction patterns (i.e., unusually complex transaction).
- Change in risk factors: Whenever there is a change in any risk factor triggered by NRA/SRA, a change in regulation or guidance, sanctions listings, or adverse media related to the customer, industry, or jurisdiction.

Customer Risk Factors:

The following are the risk factors that must be taken into consideration when conducting a comprehensive CRA:

Customer Risk	Geographic Risk	Product/Services Transaction Risk	Delivery Channel Risk	Other Risks, that may be applicable
				

[3] 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.

Examples on Risk factor categories:

Customer Risk Factors 	• Nature of the business relationship (one-off interaction (walk-in customers)/repetitive transactions/ Regular interactions or services) • Business that are cash-intensive • Use of large amounts of cash in the customer's business model/ Industry/business activities. • Non-resident customers. • The complexity of the legal, ownership or network structure of the customer (beneficial ownership transparency), Including involving of nominee shareholders, directors or bearer shares. • The type of clients the customer serves (i.e. high net worth individuals, PEPs). • Past compliance issue. Reluctance to provide information, Reluctance to disclose information or provide documents, inconsistencies in documentation, or evasive behavior during interactions • The most recent results of the National Risk Assessment ("NRA")/ Sectorial risk assessment (SRA).4 • Customers working in high-risk industries, Business Relations or Employment in High-Risk Countries, Business activity or employment involves the sale or purchase of dual-use goods, proliferation-sensitive or military goods, particularly with higher risk jurisdictions. • Adverse media screening results. • Any STR/SAR been filed against the client, UBO, or any related party.
Geographic Risk Factors 	• Engagement with clients located in/operating in, or their UBOs (nationality and residency)/source of funds from: • High-risk countries: Assess the risk of engaging with clients from countries identified as high-risk for money laundering and terrorist financing. This includes countries classified by FATF under black or grey lists, as well as those identified by the UN for terrorism financing (TF) and proliferation financing (PF). • Sanctioned countries: Engagement with clients located/ operates in countries under UN sanctions or embargoes presents heightened risks. • Countries having significant levels of corruption or other criminal activity. • Political Instability and high risk countries: Engaging with clients/ operation related to CAHRA countries (Conflict-affected and high-risk areas). areas where there is an armed conflict, a lot of violence, including violence from criminal networks, or other risks of serious and widespread harm to people. High-risk areas are those where there is a high risk of conflict or of widespread or serious abuses. Political instability or repression, institutional weakness, insecurity, the destruction of civil infrastructure, widespread violence, and violations of domestic or international law are frequently present in such areas. • Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

[4] The latest NRA/SRA reports are disseminated by the supervisory authority to entities under their supervision.

	• The above are applicable to client primary business location or headquarter, the country of citizenship or residency of the clients, the locations of incorporation or registration, the locations of linked parties and beneficial owners, and the jurisdictions from which the clients transact with the DNFBPs.
Product/service/ transaction type risk factors 	• Services that involve significant cash transactions. • Luxury and high value product (e.g. luxury and high value properties, off-shore company's formation, high value or quantity of precious stones). • Formation of Off-shore corporates. • Customer requesting to set up of a complex structure to hide the beneficial owners' identity. • Providing nominee services. • Customer dealing in dual use goods.[5] • Non-face-to-face business relationship. • Cross border transactions from high-risk jurisdictions. • A product, service or transaction that might allow for anonymity or confusion of the true identity of any of the parties involved in the transaction. • Payment received from unknown or un-associated third parties • New products and new business practices, including new delivery mechanisms or the use of new or developing technologies for a new or pre-existing product/services.
Delivery Channel Risk Factors 	• Third-Party Intermediaries: The involvement of intermediaries or agents in transactions can complicate the understanding of the transaction's true nature. This increases the risk of money laundering if the intermediaries are not thoroughly vetted. • New products and/or new business practices involving new delivery channels for new and existing products/ services, with newly developed technology. • Assessment of customer acquisition methods and/or relationship management with respect to the channel that the primary product/service is offered through. • The use of non-face-to-face channels (i.e., through electronic means), especially when the customer lacks safeguards for means of electronic identification. • Payments received from unknown or unassociated third parties. • Involvement in virtual assets • Non-Traditional Payment Methods: The use of alternative payment methods, such as cryptocurrencies or prepaid cards.
Other Risk Factors 	• Newness and/or innovation of product, service, ordelivery channel, which may not have been established in the market yet. • Assessment of operational processes with respect to cyber security, use of third parties and/or virtual assets. • The findings of the recent National/ Sectorial Risk Assessment should be taken into consideration by DNFBPs. In addition, to other reports and guidance's issued by the FATF, MENAFATF about the risks related to DNFBPs business.

[5] https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=bd550ebc-f422-47db-b104-8f67bafc6d20

The finding of the NRA/ SRA

A National risk assessment is a comprehensive evaluation carried out by a country to identify, analyze, and understand potential threats and vulnerabilities it faces from money laundering, terrorism financing and proliferation financing. The findings of these reports includes scoring the risks for each sector and highlight the most important risks factors for each sector that potentially will be more vulnerable to be misused by criminals for ML/TF/PF.

The sectoral risk assessment (SRA) is another tool that countries use to reach a more detailed understanding of the identified risks in a particular sector/subject; this assessment is usually done by the competent authorities and can include more factors/sub-sectors than a national risk assessment to build a more detailed understanding of the related risks.

DNFBPs need to consider the findings of the NRA (And/ or the sectoral risk assessment) when determining the weight for each factor to reach the final score of risks.

Applying of the Risk Based approach

The Risk Based Approach (RBA) involves that DNFBPs: identifying, assessing, and understanding the money laundering and terrorist financing risk to which they are exposed, and proactively taking the appropriate mitigation measures in accordance with the level of risk.

Implementing a Risk-Based Approach (RBA) by DNFBPs enhances the effectiveness of AML/CFT/CPF efforts by enabling a more tailored strategy for risk management. By assessing and categorizing clients and transactions based on their risk profiles. it allows DNFBPs to allocate resources more effectively by concentrating on areas with the highest risk of financial crimes. By categorizing customers and transactions based on risk profiles, DNFBPs can apply tailored compliance measures. This approach ensures that high-risk clients are subject to more stringent controls, while reducing the administrative burden for lower-risk clients.

The RBA should be reviewed and updated regularly to reflect changes in customer profiles, emerging risks, and regulatory requirements. DNFBPs should also integrate findings from the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA) into their RBA to ensure comprehensive coverage of risks at both customer and institutional levels.

Once identifying higher risk clients DNFBPs are required to implement Enhanced due diligence, the weight of some factors needs to be higher and affect the final risk score for the client, particularly when:

- Dealing with PEPs (Local, Foreign).
- Dealing with clients from FATF's Black list (High-Risk Jurisdictions subject to a Call for Action).
- Dealing with clients from FATF's Grey list (Jurisdictions under Increased Monitoring).
- New products and new business practices, including new delivery mechanisms or the use of new or developing technologies for a new or pre-existing product. Including non-face to face dealing and payment in virtual assets, ...).

By applying the RBA, DNFBPs can enhance the efficiency of their AML/CFT controls and ensure that their resources are focused on areas of greatest risk.

Steps for implementing an effective CRA?

Step 1: Define Risk Factors

Establish the factors that will be used to assess risk, this include, but not limited to (Customer Risk Factors, Geographic Risk Factors, Product/service/transaction type Risk Factors, Delivery Channel Risk Factors, Other Risk Factors, ..).

Step 2: Establish Risk Levels

Define a scale for assessing the risk levels associated with each factor. A common approach is to use a scale[6] from 1 to 5, where:

- **1** = Low Risk
- **2** = Low- Medium Risk
- **3** = Medium Risk
- **4** = Medium -High Risk
- **5** = High Risk

Example for risk scores given when dealing with Resident & Non-resident customers[7]

Factors under "Geographic Risks"	Risk Score	Factors under "Geographic Risks"	Risk Score
Non-resident from High Risk countries (FATF Black list/ Under UN sanctions)	(5)	Resident customer from high risk countries (FATF Black list)	(4)
Non-resident from Countries Under Increased Monitoring (FATF's Grey ist)	(4)	Resident customer from Countries Under Increased Monitoring (FATF's Grey List)	(3)
Non -resident from low risk countries	(3)	Resident customer from low risk countries	(2)
Non-resident holding UAE nationality	(2)	Resident customer holding UAE nationality	(1)

Step 3: Create the Risk Matrix

Set up a matrix to represent the risk levels. The matrix can have risk factors on one axis (rows) and risk levels on the other (columns).

[6] DNFBPs may decide to use 3, 4, or 6 scales of risks rather than 5.

- Example of Risk Matrix Layout

Risk Factor	Low Risk (1)	Low- Medium (2)	Medium Risk (3)	Medium -High Risk (4)	High Risk (5)
Customer Risk					
Geographic Risk					
Product/Service Risk					
Delivery Channel Risk					
other risk factors					

Step 4: Collecting of Information and documentation

Gather relevant information during the onboarding process, including identification documents, source of funds, and business activities, all al information and documentation related to the transaction.

Step 5: Assess Customer Risk/ Categorize Customers

Classify customers into risk categories based on the identified factors using the completed risk matrix of a risk scoring system.

Step 6: Calculate Overall Risk Score

DNFBPs can calculate an overall risk score by averaging the scores from each risk factor, or by assigning weight to each factor based on its importance to your institution.

Step 7: Update your controls

For higher-risk customers, to conduct EDD and apply suitable risk mitigations measures (examples of risk mitigations measures mentioned here under).

- Examples of risk Mitigation measures

Designated Non-Financial Businesses and Professions (DNFBPs) should implement a range of risk mitigation measures based on their customer risk assessments regarding Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF). Here are some key measures:

- Enhanced Due Diligence (EDD): Implement additional checks for high-risk clients, including verifying the source of funds.
- Ongoing Monitoring: Regularly review transactions for unusual activity[8] and update customer risk profiles periodically.
- Training and Awareness: Provide staff training on risks and red flags, and promote awareness of compliance policies.

[8] Unusual activity includes, but is not limited to, transactions deviating from customer transaction history, unexplained large cash deposits, and rapid movement of funds across jurisdictions.

- Robust Record Keeping: Maintaining all information, documentation, and any related investigations related to a higher-risk customer or transaction, including but not limited to EDD, analyses of suspicious transactions, and SARs/STRs, for more than 5 years is crucial.
- Updating the CRA needs to be more frequent when dealing with clients who pose a higher risk. For example, high risk: every 6 months; medium and medium-high risk: every 1 year; low-medium risk: every 1.5 years; low risk: every 2 years.
- Reporting Suspicious Activities/Transactions: Establish protocols for filing Suspicious Activity Reports (SARs/STRs) and create internal reporting mechanisms. A key aspect of this process is that when a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) is filed against a customer, their risk rating should automatically be elevated to high risk.
- Policy and Procedure Development: Develop risk-based policies tailored to specific risks and establish a governance framework for oversight.
- Know Your Customer (KYC): Implement strict customer identification and verification processes, including identifying beneficial owners. Periodically update the KYC form if any risk factors change, ensuring the collection of all necessary information for successful CRA.
- Collaboration with Authorities: share intelligence with the FIU through reporting an STR/SAR (when there is a suspicion related to financial crimes), and through sharing the trends and typologies with the related supervisory authority.
- Technology Integration: based on the risk and the size of business, using an AML software and data analytics for transaction monitoring and risk assessment could more help in implementing the CRA and suggest suitable mitigation measures with the risks identified. On the other hand, using of technology will ensure that documentation is consistent, easily accessible, and compliant with regulatory demands.

These measures help DNFBPs effectively manage and mitigate risks associated with their clients.

Step 8: Review and Update Risk Assessment

Regularly review and update the risk matrix to reflect changes in risks factors (such as, regulatory requirements, customer profile, customer behavior and emerging threats).

Step 9: Documentation

Maintain thorough documentation of the risk assessment process. DNFBPs are obliged to keep their ML/TF business risk assessment up-to-date on an ongoing basis. In fulfilling this obligation, they should review and evaluate their ML/FT risk assessment processes, models, and methodologies periodically, consistent with the nature and size of their businesses, and to make them available upon request by the competent authority.

Step 10: Compliance and Audit

A comprehensive audit trail of all customer interactions and assessments must be maintained. This should include a list of all due diligence steps, risk scores, and justifications for any actions taken.

Final conclusions

In conclusion, effective customer risk assessment is crucial for Designated Non-Financial Businesses and Professions (DNFBPs) to safeguard against Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) risks. By implementing a comprehensive and systematic approach to assessing customer risks, DNFBPs can enhance their understanding of potential vulnerabilities within their client base. This process not only aids in the identification and mitigation of risks but also ensures compliance with regulatory obligations.

It is essential for DNFBPs to continuously monitor and update their risk assessment processes, taking into account evolving threats and changes in customer behavior. Engaging relevant stakeholders, including senior management and compliance teams, will foster a culture of risk awareness and promote effective resource allocation. By prioritizing high-risk areas identified in assessments, DNFBPs can better protect themselves against financial crime while supporting their overall business objectives. A robust customer risk assessment framework will ultimately contribute to the integrity and resilience of the DNFBP's operations, ensuring a proactive stance in the fight against illicit activities.

The End