Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Counter Proliferation Financing (CPF) Supervision Guidance

Version Control:

Version	Date	Comments/Changes	Approved by
V.1	2019	Inspection Checklist-Guidance	FSRA Supervision
V.2	25 September 2022	Updated to reflect TFS Federal Requirements	FCCP
V.3	August 2024	Comprehensive review and amendments	FCCP
V.4	21 April 2025	Updated to include reference to the Supervisory Checklist on the Implementation of the Travel Rule requirements and best practices	FCCP

Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Counter Proliferation Financing (CPF) Supervision Guidance

Purpose and Scope:

The purpose of these guidelines on AML, CFT and CPF is to:

1) Provide support to Supervisors conducting assessments based on a Risk-Based Approach (RBA). This includes evaluations during onsite examinations, desk-based analyses, event-driven reviews, and thematic reviews.
2) Help assess how Firms adhere to regulatory standards as outlined in the FSRA Anti-Money Laundering and Sanctions Rulebook (AML)Federal AML legislation, and International AML standards.
3) Promote uniformity in AML, CFT and CPF findings across different assessments and reviews conducted by Supervisors.

Legal Basis:

The guidance builds upon the provisions of the following Laws and Regulations:

1) Federal Decree-Law No. (20) of 2018: Relating to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), including its amendments (referred to as the "AML-CFT Law").
2) Cabinet Decision No. (10) of 2019: As amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and the Financing of Illegal Organizations (referred to as the "AML-CFT Decision").
3) Cabinet Decision No. (74) of 2020: Concerning Terrorism Lists Regulation and the Implementation of United Nations Security Council Resolutions (UNSCRs) on Counter-Terrorism, Terrorist Financing, the Proliferation of Weapons of Mass Destruction, and related resolutions (referred to as "Cabinet Decision 74").
4) ADGM Anti-Money Laundering and Sanctions Guidance and Rules: referenced herein as the "AML Rules"

It is essential to note that this guidance is non-binding. It is designed to offer reference points and assistance rather than replicate the legal obligations specified in the AML Rules.

Frequency of Reviews:

This guidance will be reviewed regularly by the FCCP, at least once a year, to ensure it remains aligned with regulatory standards, changes and best practices.

#	References	Area	Considerations

1	Chapter 12 of the AML Rules
	
	AML12.3
	AML12.4.1
		MLRO – Appointment, qualities & responsibilities (including regulatory reporting)	Things to consider:
			• Assess the level of seniority, competence and qualities of the MLRO:
			  ○ Is the MLRO a full-time employee or is this function outsourced (including within its group)?
			  ○ Is the MLRO conducting other functions within the Relevant Person (RP)?
			  ○ Verify the MLROs reporting lines and access to the Governing Body (GB) and Senior Management (SM).
			  ○ Does the MLRO have sufficient authority and resources to carry out their role effectively?
			  ○ How engaged are the GB and SM with the AML/CFT function?
			  ○ What is the MLRO's perspective of the compliance culture within the firm?
			  ○ Assess and verify the MLRO's fulfilment of their reporting requirements to their GB / SM and to the Regulator.
			
			• Ensure a Deputy MLRO is appointed and understand the nature of the Deputy's role within the Firm.
			• Assess the adequacy of the arrangements in place in the event that the MLRO is absent.
			• The MLRO can be the Compliance Officer (CO); however, the roles of CO and MLRO would not be expected to be combined with any other Controlled Functions unless the firm implements appropriate monitoring and control arrangements independent of the individual concerned.
			
			Where relevant:
			• Interview the MLRO and Deputy, review their qualifications and review the underlying job descriptions.

			• Assess if the MLRO function is commensurate with the firm's scale of activities (including the MLRO capacity, resources, and effectiveness if outsourced (including within its group). • If outsourced, review and assess the adequacy of the existing Service Level Agreement (SLA) in place with the firm (i.e., whether the roles & responsibilities are clearly laid out, the metrics in place to measure the performance, succession measures…. etc). • Review RP's AML/CFT/CPF Policies and Procedures (P&P) and ensure the MLROs' responsibilities are up to date as set out within the AML Rules. • Review the reports submitted internally to the GB / SM and the Regulator by the MLRO (the frequency of such reports should be in line with the scale of the RP's operations. If the RP operates as a Branch in the ADGM, review the frequency of MLRO reporting to the Group on key matters). • Review the latest Annual AML Return and MLRO Report submissions. Note: • Ensure the MLRO is a UAE resident (this applies to outsourced MLROs from the Group if there is no waiver against the GEN requirement). • Ensure the MLRO is registered on the goAML system and the EOCN Sanctions alerts notification system (i.e. by verifying (1) whether the goAML profile reflects the current MLROs details and (2) EOCN alerts are being received to the registered email address).

2	AML 1.3
	AML 4.1.1 (6) (c)
	AML 12.4.2
		Governing Body and Senior Management – roles and responsibilities	Things to consider:
			• Assess the GB and SM's overall level of effectiveness, oversight, and compliance in relation to the AML risks the RP is exposed to.
			• Assess the GB's / SM's oversight over the following:
			  ○ Review and approve AML/CFT/CPF policies, procedures, systems and controls at least annually.
			  ○ Review and approve of the AML/CFT/CPF Business Risk Assessment.
			  ○ Review of regular MLRO reports including AML/CFT/CPF sanctions reports.
			  ○ Approve the AML/CFT/CPF and sanctions training programs.
			
			Where relevant:
			• Verify that the RP's GB and SM receive regular reports regarding AML/CFT and Sanctions risks (including, but not limited to onboarding, KYC, outcome of the BRA, P&Ps, PEP status, ongoing monitoring…. etc.) relevant controls and qualitative assessments of key risks that the RP is exposed to.
			• Review the Board Committee meeting packs including the minutes.
			• Oversee the periodic testing, tuning, and validation results of the transaction monitoring and sanctions screening systems.
			
			Note:
			• Verify the MLRO's involvement in the relevant AML representation and discussions within the relevant board committees.

3	AML1.3
	AML 4.1
	AML 4.2
	AML 6.1.2
	AML 6.2
	AML 8.2.2
	AML 8.3.1 (3)
	AML 10.4.1
	AML 11.1.1 (1)
	AML 11.2.1 (1) & (4)
	AML 14.2.1
	
	Cabinet Decision No. (74) of 2020
	
	Federal Law No. (31) of 2021
		Adequacy of systems and controls	Things to consider:
			• Assess whether the RP has established and maintains effective systems and controls that align with the AML Rules and Federal AML legislation.
			• Verify that the RP reviews the effectiveness of their systems and controls at least annually (refer to the independent assessment section below).
			• Verify that the RP's systems and controls in place:
			  ○ Are compliant with Federal AML legislation and ensure RP is properly informed to comply with any changes / notices / findings issued by the relevant UAE authorities and international bodies (as relevant).
			  ○ Enable it to identify, assess, monitor and manage Money Laundering (ML) risk, including the risk of Targeted Financial Sanctions (TFS) e.g., Terrorist Financing (TF), Proliferation Financing (PF).
			  ○ Are comprehensive and proportionate to the nature, scale and complexity of its activities.
			  ○ Enable it to determine whether a customer or beneficial owner is a PEP.
			  ○ Enable suspicious persons and transactions to be detected and reported.
			
			Where relevant:
			• Review AML/CFT/CPF P&P and ensure that RP maintains effective policies, procedures, systems and controls to prevent opportunities for ML/TF/PF in relation to their business and activities.
			• Ensure the systems and controls are in place and apply to all RP's branches, subsidiaries, and group entities in ADGM.
			• Ensure RP takes reasonable steps to ensure its employees comply with the systems and controls in place.
			Note:

			• In identifying its money laundering risk and establishing the necessary systems and controls, the RP should consider a range of factors, including its customer, product and activity profiles; its distribution channels; the complexity and volume of its transactions; its processes and systems; and its operating environment. The BRA will enable the RP to establish these controls and the subsequent controls required.
4	AML 4.1.1 (4) and (6)	Independent assessment	Things to consider: • Verify that the RP performs independent assessments of its policies, procedures, systems and controls at least annually. • Verify that the assessment conducted allows the RP to ensure Regulatory Compliance, mitigate risks, protect business's reputation and maintain the integrity of the financial system. • Identify and assess the frequency of the independent assessments and who conducts them (i.e. depending on the size of the firm; for large-scale firms, this may be undertaken by the Compliance Function, Quality Assurance Team, or Internal Audit. While for smaller firms, this may be carried by the MLRO or a competent firm of independent auditors or compliance professionals). • If the RP decides to outsource the review of the effectiveness of its AML/CFT/CPF policies, procedures, systems and controls, this reliance must be governed by a SLA. • Assess how the RP has considered the reviewer's suitability and independence (e.g., skills, knowledge, and experience). • Evaluate whether the assessment scope complies with the AML Rules and is appropriate relative to the firm's business activities. For instance, if the firm operates a technology-driven business model, the assessment should primarily focus on technological aspects to address specific risks. • Assess the sampling approach considered by the RP (it should be proportionate to the scale of RPs business; for example, it should consider a range of risks associated with customers' activities and transactions). Where relevant: Assess the independent assessments conducted and verify if it covers the following topics: • Review of the RP's overall adequacy of P&Ps, systems and controls. • Adequacy of customer due diligence (and enhanced due diligence), and whether they consider relevant regulatory requirements, and if the same is documented and reflected in their internal P&P. An analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; • A review of the nature and frequency of the dialogue between SM and the MLRO; • Adequacy, quality, scope, and frequency of the firm's AML/CFT assessments, including documented BRA. • Adequacy of the firm's ongoing monitoring programmes, including appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers, transactions or delivery channels and geographic locations) and the screening of customers, transactions including trade-based transactions that may involve dual-use goods, and accounts against sanctions lists. • Adequacy and effectiveness of the sanctions screening process, including UNSC and UAE sanction notifications alerts issued by the EOCN as well as those circulated by the FCCP and published on the FCCP webpage. • Assessment of the overall process for identifying and reporting suspicious transactions/activities, including a review of internal and external Suspicious Transaction/Activity Reports to determine their accuracy, timeliness, and completeness, and overall effectiveness of the firm's policy. • Review of the AML/CFT training programme to determine its comprehensiveness and effectiveness, including a review of the accuracy of materials, the training schedule, and attendance tracking; • Any other matters that the independent reviewer deems important based on the firm's nature, scale, and complexity. • Record Keeping policy. Documents to be reviewed: • RP's Compliance Monitoring Plan. • If the review is outsourced, the engagement letter between the RP and the independent reviewer. • Scope of the assessment and outcome of the review conducted. • The RP's action plan against the remediation or areas for improvement identified. Note: • The outcome of the effectiveness review should feed into the SM reporting, the management should ensure adequate oversight is exercised on the remediation of any RPs or areas for improvement identified.

<table>
<tr>
<td>5</td>
<td>Chapter 6 of the AML Rules

EOCN's Guidance on Proliferation Financing
Institutional Risk Assessment</td>
<td>Business Risk Assessment (BRA) – this includes ML, TF & PF.</td>
<td>
<u>Things to consider:</u>

Ensure RP has taken appropriate steps to identify, assess and effectively mitigate money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities.
The ML, TF & PF risks should be assessed separately.
The BRA should allow the RP to:

Understand the type of level of risk associated with its business relationships and transactions;
Determine how these risks are effectively mitigated through internal policies, procedures and controls and;
Establish the residual ML, TF & PF risks and any gaps in controls that should be addressed.
Ensure that the RPs residual risks are within its risk appetite.

Ensure RP is taking into account the following when identifying and assessing risks in the BRA:
<table>
<tr><th>Inherent Risk Factor</th><th>Consideration</th></tr>
<tr><td>Type of customers and their activities</td><td>Total number of customers, Type of customer (natural persons, legal persons, legal arrangements), Non-resident customers, PEPs, Other high-risk businesses and links to sectors commonly associated with higher levels of ML/TF/PF risk (e.g., dealers in precious metals or stones; money remitters) …etc.</td></tr>
<tr><td>Countries or geographic areas in which it does business</td><td>Countries subject to sanctions – TF and PF, FATF blacklisted/grey-listed countries, Offshore jurisdictions, Tax non-compliant jurisdictions, Countries associated with high level of corruption or organized crime, Countries associated with high TF risks</td></tr>
<tr><td>Products and services</td><td>The complexity of the product, the level of transparency of the product, service or transaction and the extent to the product, service or transaction might facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures, Private banking/wealth management, Prepaid cards, Correspondent banking services, Trade finance, Cash-Intensive Business. Etc.</td></tr>
<tr><td>Transactions</td><td>Large or Unusual Cash Transactions, International Wire Transfers, complex structuring transactions, Transactions with High-Risk Jurisdictions, Unusual Transaction Patterns, Payments for Non-existent Services or Goods, and Transactions Involving High-Risk Financial Products (e.g., cryptocurrencies or prepaid cards).</td></tr>
<tr><td>Distribution channels and business partners</td><td>Direct onboarding of customer, non-face to face onboarding of customer, use of introducers, intermediaries and/or agents, Reliance on third parties for CDD…etc.</td></tr>
</table>
Ensure that the RP assesses the relevant ML/TF/PF risks prior to the:

Development of new products and technologies.
Taking on new customers.
Changes to its business profile.

<u>Where relevant:</u>

If the BRA documentation is deficient, ask the MLRO to demonstrate how the RP has identified and assessed the vulnerabilities, and how it has captured that information and used it to mitigate the ML/TF/PF risks.
Verify the methodology or process in place for the BRA (see the note section).
Verify that the BRA updates at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and takes into consideration newly emerging threats and vulnerabilities upon the occurrence of "trigger events" such as material changes in the RP's business or risk profile or the legal and regulatory environment (e.g., takes into account the outcome of the UAE's National Risk Assessment (NRA) of AML, CFT and CPF, and any other sectoral risk assessments.)
Verify if the BRA feeds into the CRA.
Review the relevant section of the AML Return submission.
Verify if the BRA has been approved by the GB and SM.
Verify that employees are made aware of the results of BRA, for instance, through the ongoing employee ML/TF/PF training programme.

<u>Note:</u>

Ensure that the BRA is tailored to the RP and takes account of the factors and risks specific to that business. Where the RP is part of a group, the RP should ensure that the group-wide risk assessment is sufficiently granular and specific to the individual RP business and ML/TF/PF risks to which it is exposed from its operations in the ADGM.

</td>
</tr>
</table>

			• When the RP considers the outcome of the NRA (for ML, TF and PF), it should consider the overall rating considered within the NRA against the sector in which the RP is operating and assess the overall exposure and the relevant controls in place. • Frequency of review: ensure the BRA is subject to regular review to ensure it adequately reflects the ML, TF and PF risks to which the RP is exposed. At a minimum, it should be reviewed annually and upon the occurrence of "trigger events," such as material changes in the RPs business, risk profile or the legal and regulatory environment. • Ensure the BRA covers, at minimum, the following stages: o Identifying, assessing and understanding the inherent ML, TF & PF risks. o Determining the nature and intensity of risk-mitigating controls; and o Risk monitoring and review. • The BRA should form the basis of the RP's strategic operations, including: o The development of RP risk appetite in relation to AML, CTF, CPF. o The development and maintenance of AML policies, procedures, systems and controls. o Ensuring that an RP's policies, procedures, systems and controls adequately mitigate the risks to which its business is exposed. o The allocation and prioritisation of AML resources.
6	Chapter 8 of the AML Rules	Customer Due Diligence (CDD)	<u>Things to Consider:</u> • Ensure RP undertakes a RBA to identify the appropriate level of CDD and frequency of CDD in a manner proportionate to the customer's ML, TF and PF risks. • Ensure RP undertakes CDD where RP: o Establishes a business relationship with a customer. o Carries out an occasional transaction for a customer of an amount equal to or more than USD 15,000. o Suspects a customer of, or a Transaction to be for the purposes of, money laundering; or o Doubts the veracity or adequacy of any documents or information previously provided by, or obtained for, a customer in relation to the points above. • Ensure the RP has adequate systems and controls to enable it to establish business relationships with customers before verifying the identity of the customer or beneficial owner in cases where there is little risk of money laundering, and that risk is effectively managed (refer to AML 8.2). • Ensure RP applies CDD measures to existing customers, and when determining when to apply these measures to existing customers, RP to take into account (but not limited to): o Any indication that the identity of the customer, or the customer's Beneficial Owners, has changed. o Any Transactions that are not reasonably consistent with RP's knowledge of the customer. o Any change in the purpose or intended nature of RP's relationship with the customer; or o Any other matter that might affect RP's customer risk assessment. • Ensure RP undertakes Enhanced CDD for customers assigned high-risk rating. • Review a sample of RP's client files (including but not limited to verification documents obtained / identification of UBOs / nature of business relationship etc.). <u>Where Relevant:</u> • Review the relevant section of RP's P&P. • Review the relevant onboarding forms and assess how: o They facilitate the identification and verification of both natural persons and legal entities (body corporates), ensuring compliance with the requirements outlined in the AML Rules. o Evaluate the differences in documentation and requirements for different types of DD (e.g., Simplified, Standard and EDD). • Assess how the RP is validating the KYC documents. • For Body corporates, ensure the onboarding form allows the RP to identify and verify UBOs owning more than 25%. • Ensure the RP is able to adequately identify and verify any persons purporting to act on behalf of the client. • Review the relevant section of RP's AML Return. (i.e., Risk ratings, No' of customers, terminations, etc.) • Conduct sampling on the adequacy of the DD performed utilising the existing Supervision KYC Checklist. • Ensure the approval of SM is obtained when a customer is given a high-risk rating. • Where exceptions to KYC or simplified DD are exercised, the RP must document and verify the decision to perform SDD.

			Note: • CDD is the process of gathering information about a customer's identity and assessing the potential risks associated with illegal activities, such as money laundering, terrorist financing, or other illicit activities, prior to establishing a business relationship. • Screening against the UAE Local Terrorist List, UNSC Consolidated List and other relevant lists must be completed at this stage. • Ensure RP maintains a record of a copy of all documents and information obtained in undertaking initial and ongoing CDD or due diligence on business partners. • Ensure RP's systems and controls in place take reasonable measures to identify PEPs. • For clients who are trusts and/or foundations, refer to the relevant sections of Chapter 8 of the AML Rules and the specific requirements that RP should consider. • Where identity verification is performed without face-to-face contact, an RP should make additional checks to manage the risk of identity theft and fraud. The additional checks may consist of robust anti-fraud checks that the RP routinely undertakes as part of its existing procedures, which may include: o Reliance on the UAE Pass to identify and verify the identity of a customer who is a Natural Person, and thereby satisfying the requirement to verify the address of that customer only where the RP has duly authenticated the UAE Pass; or o Deploy digital identity verification solutions that enable the RP to rely on facial recognition and other biometric data to confirm a client's identity.
7	Chapter 7 of the AML Rules	Customer Risk Assessment (CRA)	Things to consider: • Ensure the RP: o Conducts a risk assessment based on factors such as customer type, geographical location, nature of the business relationship, delivery channels and transaction volume. o Determine the risk rating of the customer (e.g., low, medium, high) based on their risk profile, business, and transaction patterns. o Establishes a schedule for periodic review of customer profiles based on risk assessment (e.g., annually for low-risk customers and more frequently for high-risk). • Verify if the CRA is completed: o Prior to establishing a business relationship with a customer. o On a periodic basis, upon KYC reviews or changes to a customer's information. o Whenever is it appropriate for existing customers (i.e. changes to the risk factors associated with the customer). • Verify if the RP's risk-based assessment of a customer identifies, assesses, and considers: o The customer and any beneficial owners. o Purpose and nature of the business relationship and the nature of the customer's business. o Customer's country of origin, residence, nationality, and place of incorporation or business. o The relevant product, services or Transaction. o The outcomes of the BRA in terms of product, services or transaction. • Verify if RP maintains and updates its list of customers (either manually or within a system). • Verify if the degree of CDD conducted for a customer is in line with the allocated risk rating. • Verify the assessment undertaken against clients, and the adequacy of the documentation (i.e., the MLRO should document the reasons for the overall risk rating assigned and the level of due diligence). Where relevant: • Identify whether the RP has outlined the CRA methodology in its P&Ps. • Review the adequacy of the CRA methodology and whether it's designed to assist in allocating a risk rating to a client. The methodology should include, at minimum, the identification of risks, risk assessment criteria (e.g., risk categories, scoring grid, weighting) and risk mitigation and controls. • The RP should maintain a country risk rating document or repository such as the FATF and Basel AML index of Know Your Country when assessing the geographical risks associated with clients. The country risk rating document should take into consideration the Decision by the National Committee for Combating Money Laundering and Financing Terrorism and Illegal Organisations (the Committee) regarding High-Risk Jurisdictions. • Assess the effectiveness of the relevant controls in place in relation to rejections and/or terminations of prospective and existing customers due to the implementation of a risk-based approach, this can involve the review of the following: o The relevant sections in the AML Return (i.e. Risk ratings, No' of customers / terminations, etc.). o The RP's log for the number of prospective and existing customers that were terminated or rejected along with the reasons (e.g., Sanctions, not within the firm's risk appetite, Adverse Media, Incomplete CDD, Non-Identification of UBO, Inaccurate documentation, Inadequate KYC documentation, unclear Source of Wealth, Fake documents…. etc). Note:

			• Risk ratings should be descriptive (e.g., low/medium/high or score of 1-5) and determine to what degree CDD will need to be performed in accordance with the client risk profile.
			• The screening conducted on the client (including adverse media and PEP identification) should feed into the overall risk rating.
			• A Relevant Person must not:
			  ○ Establish a correspondent banking relationship with a Shell Bank;
			  ○ Establish or keep anonymous accounts or accounts in false names; or
			  ○ Maintain a nominee account held in the name of one person, but controlled by or held for the benefit of another person whose identity has not been disclosed to the Relevant Person. Ensure that the RBAs are clear, rational and comply with the requirements of AML 7.2.1(5).
			• For further details on how RBAs should be conducted and how they relate to the CDD process, see guidance of section 7.1.

8	AML 8.4	Enhanced Due Diligence (EDD)	<u>Things to Consider:</u>
			• When a customer relationship is deemed high risk, the RP must obtain:
			  ○ Additional identification information on the customer and all Beneficial Owners, such as whether the customer is a PEP or related to one and if the entity has a complex ownership structure, information on the purpose and legitimacy of the complex structures to ensure that they are not used to obscure true ownership or control.
			  ○ Additional information on the intended nature of the business relationship, such as: why they are seeking RP services and how they intend to use them.
			  ○ Information on the reasons for a transaction, such as the nature of anticipated transactions, including the expected volume, frequency, and types of transactions.
			  ○ And identify / verify:
			  ▪ Source of Funds – able to verify the legitimate source of the customer's and its UBOs' funds used in transactions.
			  ▪ Source of Wealth – able to determine the origin of the customer's and its UBOs' total wealth or assets.
			• Update the CDD information which it holds on to the customer and any Beneficial Owners more regularly (this should be based on the underlying RBA).
			• Conducts enhanced monitoring of the business relationship, client profile and transactions at least annually or more frequently as deemed by the RP.
			• Obtains the approval of SM to commence a business relationship with the customer.
			
			<u>Where relevant:</u>
			• Review the relevant EDD section of RP's P&Ps.
			• Determine the EDD requirements or parameters for higher-risk customers, for example:
			  ○ Customer Risk Factors: Cash-intensive business, PEP (or close relatives), nature of PEP (domestic or foreign), non-resident customers, correspondent banking relationship, complex ownership structures …etc.
			  ○ Geographical risk factors: High-risk countries or countries with inadequate AML Controls, customers from high-risk jurisdictions…etc.
			  ○ Product/service risk factors: if the client's business operations are in sectors which are deemed high: precious metals, charities, Export-Import Trade, High-Value Goods and Luxury Assets…. etc.
			  ○ Transaction or delivery channel risk factors: transactions involve multiple parties or multiple jurisdictions, transactions linked to jurisdictions with high money laundering or terrorist financing risks, or those identified by FATF or local regulators as high-risk, Non-Face-to-Face relationship, payment from third party…etc.
			  ○ Others: Customers with Unusual or Suspicious Behaviour (such as frequent changes in transaction patterns, use of third-party intermediaries, reluctance to provide information, Adverse Media or Negative Information…etc).
			• Verify RP's degree of DD in relation to high-risk customers.
			• Verify if the RP has in place predefined thresholds for certain transaction parameters (e.g., large amounts, frequent transactions or deviations from expected patterns or anomalies that could indicate suspicious activity).
			
			<u>Note:</u>
			For EDD, a declaration cannot be considered an independent or reliable verification source, and hence, necessary documents must be sought to establish its legitimacy.

9	AML 8.1.2 (1) AML 8.6	Ongoing Customer Due Diligence	<u>Things to consider:</u> • Verify that the RP conducts ongoing CDD and the frequency of CDD conducted (in cases of but not limited to periodic reviews, unusual Transactions, changes in business relationships, changes in customer information…. etc.) • In relation to ongoing CDD, Ensure RP:

			○ Periodically reviews the adequacy of the CDD information it holds on customers and Beneficial Owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating. ○ Periodically review each customer to ensure that the risk rating assigned to a customer remains appropriate for the customer in light of the ML, TF & PF risks. ○ Monitor Transactions undertaken during the course of its customer relationship to ensure that the Transactions are consistent with the RPs knowledge of the customer, his business and risk rating. ○ Pay particular attention to any complex or unusually large Transactions or unusual patterns of Transactions that have no apparent or visible economic or legitimate purpose. ○ Enquire into the background and purpose of the above transactions. ○ Review a sample of RP's periodic client file reviews (this could be combined with the client file reviews referenced in Customer Due Diligence (CDD) section). Where relevant: • Review the relevant section of RP's P&Ps relevant to the ongoing CDD reviews (interview the MLRO to determine whether P&Ps regarding ongoing CDD are adhered to). • Review the relevant section of RP's AML Return in relation to ongoing CDD. • Where the RP relies on advanced technology to automate the ongoing CDD process, assess how these are carried and the adequacy of the controls in place. • Review client files to assess the adequacy of ongoing CDD undertaken, especially in cases of high-risk customers. • Review the trigger events that require reviewing a customer's KYC information. • Verify how often KYC is refreshed for clients including maintaining up to date information on their clients (i.e., identification documents). Note: • The ongoing CDD process involves customer identification and verification, risk assessment, transaction monitoring, and periodic review of customer information.
10	Chapter 9 of the AML Rules	Reliance on a Third Party / Business Partner Identification	**Reliance on a Third Party for CDD:** Things to Consider: • Whether the RP outsourced CDD (including sanction screening and transaction monitoring) to a third party and, if so, if the party meets the obligations under the AML Rules. • Verify whether the outsourced party is subject to regulation, is in line with and considers AML/CFT/CPF standards (including but not limited to FATF standards). Where relevant: • Review the outsourcing agreement in place. • Verify how RP made its assessment in relation to the outsourced party and if records of those assessments were kept. • Verify if RP conducts periodic assurance assessments of the outsourced party. • Verify if RP promptly requests material in cases where it lacks sufficient information or documentation. Note: • In cases of reliance on third parties, ensure RP relies on the following to conduct one or more elements of CDD on its behalf: ○ Authorised Person or Recognised Body. ○ Law firm notary, or other independent legal business, accounting firm, audit firm, insolvency practitioner or equivalent in another jurisdiction. ○ Financial institution. ○ A member of RP's group ○ Other specialized utilities for providing outsourced AML/CFT/CPF services. • RP may rely on information previously obtained from a third party which covers one or more elements of CDD. • RP remains responsible for compliance with CDD rules/regulations, regardless of whether the CDD process is in-house or outsourced. • Ensure that the RP immediately undertakes the CDD directly if it becomes aware of any deficiency in the third party's CDD efforts.

			Business Partner[1] Identification:
			Things to consider
			• Whether the RP:
			  ○ Verifies the identity of its business partners by obtaining sufficient and satisfactory evidence.
			  ○ Maintains accurate and up-to-date information and conducts ongoing due diligence. In case, RP becomes aware that it lacks sufficient information or documentation concerning a business partner's identification or develops a concern about the accuracy of its current information or documentation, it must promptly obtain appropriate material to verify such business partner's identity.
			  ○ Documents what due diligence has been undertaken by the third-party.
			
			• In cases where RP operates or maintains a Correspondent Account for a Correspondent Banking client, verify if it has arrangements to:
			  ○ Conduct due diligence with respect to the opening of a Correspondent Account for a Correspondent Banking client.
			  ○ Identify all third parties that will use the Correspondent Account.
			  ○ Monitor Transactions processed through a Correspondent Account that has been opened by a Correspondent Banking client to detect and report any suspicion of ML.

11	Cabinet Resolution No. 74 of 2020
	
	Chapter 11 of the AML Rules
		Targeted Financial Sanctions (TFS): **Legal Requirements in UAE**	Targeted Financial Sanctions (TFS) are restriction measures mandated by the UAE, requiring RPs to freeze the funds and other assets of any current or potential customer whose name appears on any of the following lists:
			• Local lists, including UAE's local terrorist lists issued by the Cabinet and sanctions lists featuring names of individuals and entities associated with the Financing of Terrorism or Proliferation Financing of weapons of mass destruction.
			• Sanctions lists issued by United Nations Security Council Resolutions (UNSCRs) – referenced herein as the "UN Consolidated List"
			
			Therefore, Supervisors should verify that the RP is adhering to the following requirements related to TFS:
			  ○ That the RP is registered on the Executive Office for Control & Non-Proliferation (EOCN) notification system to receive timely and regular updates from the UN Security Council, the sanctions committee, or the UAE's Local Terrorist List about new listings, re-listings, or de-listings.
			  ○ Conduct regular and ongoing screening of transactions and databases to check for name matches against the sanctions list mentioned above.
			  ○ RP is aware of the requirement to:
			  ○ Submit the mandatory TFS survey following each sanction alert notification received by the EOCN;
			  ○ Apply freezing or suspending measures, without delay (within 24 hours), all funds or other assets upon identification of confirmed or potential match and refrain from providing any services in line with Cabinet Resolution No. 74 of 2020; and
			  ○ File the relevant reports through the goAML; Funds Freeze Report (FFR) and Partial Name Match Report (PNMR).

12	Cabinet Resolution No. 74 of 2020 Chapter 11 of the AML Rules	TFS – Policies & Procedures (P&P)	Things to consider: • Whether there are documented procedures for screening customers and all related parties against the UAE Local Terrorist List, and UNSC Consolidated List. • Whether there are documented procedures for actioning freezing orders; • What methods are used to screen customers and related parties during the customer onboarding process and who undertakes this function; • Whether the Firm's procedures incorporate further analysis when a positive hit is returned and verify that it is clearly outlined who is responsible for determining if the hit is a false positive. • Whether screening is undertaken on an ongoing basis and at what frequency. Where relevant: Review RP's P&P related to TFS and ensure that it adequately covers the following aspects: • GB and SM roles and responsibilities concerning TFS. • Description and frequency of the management information system reports for the GB and SM. • The roles and responsibilities of the Sanctions screening function, including ownership and accountability for each stage of the process (this would apply to for large-scale firms). • The different types of screening conducted by the RP (such as name screening and transaction screening) and the information that is screened for each type.

[1] Includes: Authorised Person or Recognised Body, law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent Person in another jurisdiction, FI, member of the Relevant Person's Group, other specialised utilities for the provision of outsourced AML/TFS services, or a Correspondent Bank.

			• Description of the different circumstances where screening is conducted (i.e., prior to onboarding new customers, employees, and services providers, and upon KYC reviews or changes to a customer's information). • Description of what the RP screens (i.e., customer databases, names of parties to any transactions, UBOs, individual client/legal entity name, controllers, directors and/or agents acting on behalf of customers...etc). • The process and frequency of data testing, tuning, and validation of the sanctions screening systems. • List management processes and practices. • Sanctions screening alert review and escalation processes. • Asset freezing processes and practices. • Internal investigation process. • Request for information (RFI) process. • Assess and review the resources assigned to TFS, including sanctions screening, and ensure that the roles and responsibilities of TM functions are clearly defined and documented. • Verify that employees are required to read and sign off the TFS P&P. <u>Documents to be reviewed:</u> • TFS P&P • Organization Chart and list of TFS function employees (for large-scale firms)

13	Cabinet Resolution No. 74 of 2020
	
	Chapter 11 of the AML Rules
		TFS – systems and controls	<u>Things to consider:</u>
			• Has the RP established adequate controls to identify, assess and monitor violations of TFS?
			• Conduct a walkthrough to determine the effectiveness of the sanctions screening and whether the transaction monitoring process is automated or manual.
			• Where a firm has used an external technology application/solution – how does the firm ensure that screening parameters and outputs are in line with Federal requirements?
			• Confirm the frequency at which the RP screens the customer database (regularly).
			• An RP must verify that screening is conducted in the following circumstances (i.e. when):
			  ○ Upon any updates to the Local Terrorist List or UN Consolidated List. In such cases, screening must be conducted immediately and without delay to ensure compliance with implementing freezing measures without delay (within 24 hours).
			  ○ Prior to onboarding new customers.
			  ○ Upon KYC reviews or changes to a customer's information.
			  ○ Before processing any transaction (Name Screening).
			• Verify that RP conducts screening on the following parties (i.e. who):
			  ○ Existing customer databases – all systems containing customer data and transactions need to be mapped to the screening system to ensure full compliance.
			  ○ Potential customers before conducting any transactions or entering a business relationship with any Person.
			  ○ Names of parties to any transactions (e.g., buyer, seller, agent, sender, receiver, etc.)
			  ○ Ultimate beneficial owners, both natural and legal.
			  ○ PEPs.
			  ○ Names of individuals, entities, or groups with direct or indirect relationships with designated persons.
			  ○ Directors and/or agents acting on behalf of customers (including individuals with power of attorney).
			• Ensure that the RP conducts periodic testing, tuning, and data validation of the screening system, which should at least cover the following:
			  ○ The integrity, accuracy and quality of data sources feeding into the screening system and system output.
			  ○ The adequacy of the name-matching algorithm.
			  ○ Review an example of a recent notification and discuss the process of screening customer databases and submitting the TFS mandatory survey after the screening.
			• Verify whether the RP has incorporated a quality assurance process into its sanctions screening process.
			
			<u>Documents to be reviewed:</u>
			• If screening is outsourced, a copy of the confirmation of the existence of an SLA is to be reviewed to ensure and verify the controls employed by the vendor (i.e. list source (should include the UAE Local Terrorist List & UN Consolidated List) and the frequency of updates (i.e. any updates to the UAE Local Terrorist List & UN Consolidated List should not take more than 24hours to be reflected within the underlying source list).

<table>
<tr>
<td>14</td>
<td>Cabinet Resolution No. 74 of 2020

Chapter 11 of the AML Rules</td>
<td>TFS – alert management system</td>
<td>
<u>Things to consider:</u>

Review the alert management system with respect to sanctions screening.
Review and assess the adequacy of escalation processes.
Ensure relevant staff are aware of the operation of the sanctions screening system and escalation process.
Review a sample of alerts generated by the sanctions screening system to ensure that the level of review conducted is satisfactory. Assess whether the following aspects are considered when discounting an alert:

<table>
<tr><th>Natural Persons</th><th>Legal Persons</th></tr>
<tr><td>Name
Aliases
Date of birth
Nationality
ID or passport information
Last known address</td><td>Name (s)
Aliases
Address of registration
License/registration number
Address of branches</td></tr>
</table>
<u>Where relevant:</u>

Ensure that RP adopts effective management practices for sanctions lists by considering, at minimum, the following aspects:

List management selection;
Sourcing of lists;
List maintenance;
Whitelisting/de-listing;
Fuzzy logic; and
Data quality of underlying customer data.

<u>Documents to be reviewed:</u>

The register of all sanctions screening hits (negative, potential, and confirmed matches) generated over a specific period (e.g. period to be selected based on the number of hits).
If available, request the latest quality assurance review outcome conducted to assess the effectiveness of screening measures.
An example copy of the latest mandatory TFS survey conducted following a sanction alert notification.

</td>
</tr>
<tr>
<td>15</td>
<td>Cabinet Resolution No. 74 of 2020

Chapter 11 of the AML Rules</td>
<td>TFS – positive match & asset freeze</td>
<td>
<u>Things to consider:</u>

Ascertain that the RP reports without delay all confirmed or potential matches related to any persons or entities designated pursuant to any "positive hit" in the context of UN Consolidated List and UAE Local Terrorist. This includes:

Report any confirmed match by raising a Funds Freeze Report (FFR) via GoAML within 5 business days from implementing any freeze measures.
Report any potential match by raising a Partial Name Match Report (PNMR) via GoAML within 5 business days from implementing any suspension measures.
Any suspicious transactions or activities that do not include confirmed or potential matches to the UAE Local Terrorist List or UN Consolidated List should be reported to the FIU by raising a FFR/PNMR through the goAML platform, should contain sufficient and good quality information.

Verify that the RP maintains a record of false positives discovered during the screening process on the UAE Local Terrorist List or UN Consolidated List.
Ensure that RP maintains records of all screening results (negatives, false positives, potentials, and confirmed matches) for at least six years.
When submitting FFRs or PNMRs, verify that the RP includes the following minimum required documents:

ID documents of confirmed / potential match (and any related parties to the transaction).

Natural person: National ID and/or Passport & Residency Visa.
Legal person: Trade License, Memorandum of Associations, etc.

Specify the total amount frozen / suspended, including proof documents (e.g., bank statements, transaction receipts, securities portfolio statement, etc.).

Verify that RP responds to communications (queries, requests for information, etc.) received from EOCN via goAML message board within 48 hours of receiving the communication.

</td>
</tr>
</table>

			• Verify that RP implements the freezing, cancellation, or lifting of freezing measures for other assets immediately upon confirmed or potential match identification and (within 24 hours) pursuant to related UN Consolidated List or Cabinet Decisions regarding issuance of the Local Terrorist List and without prior notice to the designated individual, entity, or group. Documents to be reviewed: • The register of all sanction screening notification alerts, including data on receiving the alert, classification of alert (e.g., freezing, cancellation, or lifts freezing), date of screening, and their status of screening (positive, negative hit/match), raised report to goAML (e.g., FFRs and PNMRs).
16	Guidance under section 8 of the AML Rules Decision by the National Committee for Combating Money Laundering and Financing Terrorism and Illegal Organisations (the Committee) regarding High-Risk Jurisdictions	Transaction Monitoring (TM) – systems & controls	Things to consider: • The form and method of monitoring and if it is appropriate given the nature, scale and complexity of the Firm, this includes: o Whether transaction monitoring is manual or automated; o RPs with larger operations are anticipated to have automated systems that can manage the risks associated with a higher volume and variety of transactions. o The frequency and scope of transaction monitoring (are all transactions reviewed/filtered); • Whether transaction/activity monitoring is conducted against the customer profile of expected activity; • The RP transaction threshold should consider at minimum the following: o Be reasonable to the client base & business model. o Rules or scenarios should be built on previous customer behaviour trends and linked to volume and location of transaction (e.g. where is this transaction instruction coming from? If from a sanctioned country this should be flagged, or multiple people access to different accounts). o Country-specific scenarios should be built if the RP processes cross-border transactions. o Consider UAE typology reports relevant to its operations. o Set rules to flag large transactions that are inconsistent with the customer's known financial profile or business activities. o Rules to detect patterns of frequent or unusual transactions that deviate from a customer's typical behaviour. • Verify that the RP implemented EDD measures on all Transactions (for example: trade transactions and stricter thresholds for high-risk transactions or customers, considering specific risks and typologies associated with their profile). • Has the RP established internal procedures to ensure that customers have a valid permit when dealing in export and import of dual-use items before processing transactions or engaging in business relations? Where relevant: • Review RP's P&P related to TM and ensure that it adequately covers the following aspects: o GB and SM roles and responsibilities. o Description and frequency of the management information system reports for the GB and SM. o The roles and responsibilities of the transaction monitoring function. o The rules/scenarios used in the transaction monitoring system, including risk factors, parameters and thresholds. o The process and frequency of testing, tuning, and validation of the transaction monitoring system. o Transaction monitoring alert review and escalation processes. o Internal investigation process. o Request for information (RFI) process. o SAR and STR Reporting. • Review and assess: o If the MLRO, Deputy MLRO or specific team is responsible for monitoring and reviewing flagged transactions or activity for further examination. o If manual monitoring is implemented, evaluate/assess the training on transaction monitoring policies and procedures to ensure that business-line employees follow internal processes for identifying and referring potentially suspicious activities. o Whether RP's TM systems can detect potentially suspicious or illegal activity patterns across multiple transactions. o If the Firm has procedures for conducting enhanced monitoring for higher risk customers, products or services and what this entails; and o Whether complex, unusually large transactions or transactions that have no apparent or visible economic or lawful purpose are examined. Consider how these are detected and who they are examined by. o Red flags relevant to the business activities of the firm, such as: the size of the transaction in comparison to the customer's profile, large deposits, money transfers, etc. o Review/assess the adequacy of the resources assigned to TM and ensure that the roles and responsibilities of TM functions are clearly defined and documented. o Conduct a walkthrough to assess the effectiveness of the transaction monitoring system.

			• If the TM process is automated, ensure that the RP conducts periodic testing, tuning, and data validation of the transaction monitoring system, covering at least the following aspects:
			  ○ The adequacy of the detection rules/scenarios, parameters and thresholds.
			  ○ The integrity, accuracy and quality of data sources feeding into the transaction monitoring system and system output. RP should identify and document all data sources that serve as inputs into their TM program.
			  ○ Frequency of data testing and validation:
			  ▪ such testing may include data integrity checks to verify that data is being fully and accurately captured in source systems and transmitted to transaction monitoring systems.
			  ▪ In addition, when introducing new rules, RP should undertake pre-implementation testing of transaction monitoring rules and systems, employing historical transaction data as appropriate.
			  ○ The adequacy of the risk-weighted scoring mechanism and the application of a risk-based approach.
			
			<u>Documents to be reviewed:</u>
			• TM P&P
			• The latest TM system assessment report, including the scope and outcome of the review.
			
			<u>Note:</u>
			• RPs are required to report High-Risk Country Transaction Report (HRC) and High-Risk Country Activity Report Activity (HRCAR) through the FIU goAML when observing transactions or activities related to high-risk countries subject to a Call for Action, by FATF.

17	Guidance under section 8 of the AML Rules	TM – alert management system	<u>Things to consider:</u>
			• Review the alert management system and alert scoring process to determine the RP's risk-based approach to TM.
			• Review and assess the adequacy of alert adjudication and escalation processes.
			• Ensure that all relevant staff members are aware of the operation of the TM system, the alert adjudication process, and the escalation process.
			• Review a sample of alerts generated by the TM system to ensure that the level of review performed is satisfactory. Assess whether the RP considers the following aspects when reviewing an alert:
			  ○ The customer information is maintained in the client file.
			  ○ Conduct internet searches.
			  ○ Obtains additional information from the client.
			  ○ Review previous transactions and account activities.
			
			• Confirm that the RP has an embedded quality assurance process within its transaction monitoring program.
			• Ensure the RP assesses the age profile for reviewing/outstanding alerts to determine if there is a backlog. If backlog exists, understand the reason of backlog (e.g., efficiency of the TM system, lack of resources…etc)
			
			<u>Documents to be reviewed:</u>
			• The register of all TM alerts generated within a specific period (preferably over a quarter, depending on the volume of transactions) should be selected as a sample for review.
			• If available, request the latest quality assurance review outcome.

18	Chapter 14 of the AML Rules	Suspicious activity/transactions report (SAR/STR) – Controls	<u>Things to consider:</u>
			• Review RP's P&P related to SAR/STR and ensure that it adequately covers the following aspects:
			  ○ The roles and responsibilities of the individuals involved in the SAR process.
			  ○ Description of the internal SAR/STR process.
			  ○ The internal SAR/STR template(s).
			  ○ Description of the internal investigation process and reports.
			  ○ Explanation of the external reporting process.

			• Whether the Firm's procedures include actions to take following a SAR/STR filing to the FIU, including notification to the Regulatory Authority, preventing tipping off, what to do if a customer wishes to move their funds, etc.; and
			• The register of SAR/STR should include, at minimum, the following:
			  ○ The individual or team referring the suspicious activity or transaction to the MLRO for review.
			  ○ The time and date of the suspicious transaction or activity.
			  ○ The parties involved in the transaction.
			  ○ The location where the transaction occurred.
			  ○ The red flags or reason for suspicion identified.
			  ○ The action taken by the RP (e.g. assessed and closed, or external SAR/STR was filed).
			
			Where relevant:
			• Understand how employees are able to identify suspicious activity;
			• How the Firm ensures staff are aware of the tipping-off offence;
			• Whether employees understand their obligations to make internal reports to the MLRO of any suspicious transaction/ activity;
			• The level of detail of the Firm's internal procedures for reporting potentially suspicious transactions (e.g. timeframes, approvals, use of a template report for internal suspicious transactions, etc); and
			• How employees are made aware that failing to make a report may result in disciplinary action.
			• Verify that employees are required to read and sign off the AML P&P.
			• Whether there are documented procedures for the MLRO to follow on receipt of an internal STR/SAR;
			• How the MLRO documents the investigation; and
			• Evaluate whether the MLRO has the authority to independently decide whether to report to the FIU, without the need for consent or approval from any other person).
			
			Documents to be reviewed:
			• SAR/STR P&P (these can be contained within the overarching firm's policy).

19	AML 14.2	SAR/STR – Internal report	Things to consider: • Does the RP properly investigate, document and report internal SAR/STRs? • Ensure that the RP has a clear process for handling and recording suspicious activities/transactions internally, and reporting them through the goAML system • Ensure that the RP's handling of internal SAR/STR meets the minimum requirements of AML 14.3.1, and that the related documentation complies with AML 14.3.2 and 14.3.3. Documents to be reviewed: • The register of internal SAR/STR. • The internal SAR/STR template(s) Note: • The internal log should also indicate the number and when an external SAR/STR is filed and provide reasons for instances where such reports were not made. Review any meeting minutes or Internal reports that documents such actions.
20	AML 14.3	SAR/STR – external report	Things to consider: • Does the RP properly investigate, document and report external SAR/STRs through goAML? • Ensure that the RP has a clear process for handling, recording, and reporting internal SARs/STRs. • Ensures that external SAR/STRs have not been subject to the approval of any person besides the MLRO: AML 14.3.4. • Ensure that the external SAR/STRs are complete, sufficient and timely filed in the goAML system. Where relevant: • Review a sample of external SARs/STRs to assess their quality. • Review the relevant sections of the AML Return.

			Documents to be reviewed: • The register of external SAR/STR. • Review any meeting minutes or external reports that documents such actions.
21	Chapter 13 of the AML Rules	Training & awareness	Things to consider: • Ensure RP: o Has a documented training programme including the scope and content of AML, CFT and CPF training, including frequency, delivery methods and provider; o Whether training is tailored for different employees; o Conduct adequate internal training and awareness on AML, CFT and CPF obligations and sanctions evasion typologies to relevant staff and senior management (e.g., Board of Directors, Senior Management, MLROs, Front Desk Staff, Relationship Managers, Compliance Officers, etc.). o Whether employees are required to undertake AML, CFT and CPF training before undertaking customer-related or other relevant activities; o Whether the training material is reviewed at regular intervals to assess if it remains fit for purpose and meets the business needs; and o Whether and how employees are assessed for knowledge retention following the AML/CFT training. • Ensure that RP's AML, CFT and CPF training enables its employees to: o Know the identity and understand the responsibilities of RP's MLRO and Deputy MLRO. o Understand the relevant AML legislation (including Federal AML legislation). o Understand its P&Ps, systems and controls related to ML, T F & PF and any changes to these. o Recognise and deal with transactions, risks, trends, techniques, and other activities related to ML, TF and PF. o Understand the types of activities/transactions that may constitute suspicious activity. o Understand its arrangements regarding making an internal notification to the MLRO of suspicious activity. o Be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of RP. o Understand the roles and responsibilities of employees in combatting ML, TF and PF. o Understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices etc. • Ensure RP maintains a training log which includes: o Dates the training was given. o Nature of the training. o Names of the employees who conducted / received the training. Where relevant: • Review RP's Training materials. • Review RP's Training logs which should cover all the AML, CFT and CPF training sessions attended held by EOCN, SSC and/or Supervisory Authorities. • Review RP's training policy. • Verify if RP's relevant staff have attended AML/CFT/CPF training sessions conducted by ADGM and Federal Authorities. Note: • Training logs / records must be kept for at least six years. • In addition to the ML training, the TFS training and awareness should cover obligations under Article 21 of Cabinet Decision No. 74 of 2020, as well as reference to "Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs" published by EOCN and any other TFS guidance published by the EOCN and/or Supervisory Authority. RPs may also utilize the "Targeted Financial Sanctions Training Presentation" published on the EO IEC website for internal use.
22	AML 4.5 AML 12.4.2 (c) AML 13.3 AML 14.3.3 AML 14.5 AML 16.2	Record Keeping	Things to consider: • The adequacy of record retention includes the form in which records are maintained (hard copy, electronic), whether they are maintained onsite in the ADGM office or at another location and can information be readily accessed and obtained; • Whether documents are in English, and if they are available in a language other than English, an appropriate translation is to be maintained; • Whether the requirements for record keeping are documented; and • If records are maintained outside the ADGM, the appropriateness of those arrangements and whether there are any secrecy or data protection legislation that may restrict access. • Ensure RP maintains records of the following (not limited to): o Copy of all documents and information obtained in undertaking initial and ongoing CDD.

			○ Records consisting of the original documents or certified copies in respect of the customer business relationship. ○ Records of sanctions screening conducted and hits identified. ○ Internal notifications of suspicious activity made to its MLRO. ○ SAR/STR reports and any relevant supporting documents and information, including internal findings and analysis, and any relevant communications with the FIU. ○ Copy of the submitted AML Returns. ○ AML/CFT/CPF Trainings (including materials & log). Where relevant: • Review the section pertaining to record keeping within the RP's P&P. • Ensure the record keeping requirements are aligned with the required records set within the AML Rules. • Ensure the retention period is for at least six years (or whichever is greater depending on if the RP is part of the Group and has to comply with legislation imposed on its Group). • Verify RP's promptness and cooperation in providing records to the regulator (expectation of receipt within one Business Day from the request). • Review the method or manner in which the records are kept (i.e., its form (electronically), accessibility, and readiness when requested). Note: • RP must ensure records are kept regardless of whether or not it is outsourcing an element of its CDD process.
23	AML10.3	Wire transfers and the Travel Rule	Things to consider: • Ensure that AP is familiar with the Travel Rule obligations-according to the FATF Recommendation 16 and its subsequent implementation updates. • Ensure AP complies with requirements to obtain, hold, and transmit securely and without delay originator and beneficiary information (e.g., Originator's name, Originator's account number or a unique transaction reference number, originator's address (or national identity number, or travel document number, or customer identification number, or date and place of birth), Beneficiary's name and Beneficiary's account number or a unique transaction reference number). • Ensure the AP has a mechanism to securely and promptly transmit the required information to other VASPs or financial institutions. • Ensure that AP verifies the accuracy of the information collected under the Travel Rule as relevant (pay attention to inward and outward transactions with un-hosted wallets) • Verify if the AP maintain records of the information collected and transmitted as per the Travel Rule. • In case there is "Batch Transfers"- ensure the AP verifies the originator information, and that the batch file contains the beneficiary information for each beneficiary and that the information is fully traceable in the beneficiary's jurisdiction. • Ensure that AP monitors for, and conducts enhanced scrutiny of, suspicious activities, including incoming transfers that do not contain complete originator information, including name, address and account number or unique reference number. • Ensure AP implements appropriate rules and logic in their systems to ensure that no transfer is processed without including identification details for both the originator and the beneficiary. • Ensure that the AP has adopted a Travel Rule technological solution to identify counterparty VASPs and to ensure compliance with the Travel Rule. • Ensure that no de minimis threshold is applied to the size of a relevant transfer when complying with the Travel Rule. • Ensure that AP conducts Due Diligence on counterparties in compliance with R.16 and the AML Rules. • Ensure that AP's employees are all aware of and trained on the requirements of the Travel Rule. Where relevant: • Review samples of transactions to ensure that the AP complies with the requirements of AML 10.3.2(1) and 10.3.2(3) when processing transfers. These should include records of all transfer transactions including the originator's and beneficiary's information, amounts, dates, and any relevant notes or memos. • Review copy of the firms' policies and implemented procedures for complying with the Travel Rule. ***To further support the effective implementation of the Travel Rule, supervisors can refer to the Supervisory Checklist referenced under Appendix A on the Implementation of the Travel Rule requirements and best practices which equips supervisors with the necessary framework to comprehensively address the Travel Rule aspects of VASPs while taking into consideration FATF guidance and best practises.***

24	AML 4.4 AML 4.7	Notifications and Cooperation with other Regulators	Things to consider: • Ensure that whenever the RP receives a request for information from a Non-ADGM Financial Services Regulator or agency responsible for AML regarding enquiries into potential Money Laundering related to Regulated Activities carried on in or from the ADGM, must promptly inform the FSRA in writing. • Ensure that whenever the RP becomes aware, or has reasonable grounds to believe, that the following has or may have occurred in or through its business money laundering contrary to relevant Federal AML Legislation (e.g., a breach of Sanctions, or acts of bribery under the OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions). Where relevant: • Review the RPs P&P to ensure they cover the above obligations. • Review the tracking log to check if the MLRO and SM have received any requests or suspected leads that require the RP to notify the FSRA.

Appendix A:

Checklist - Travel Rule requirements a