AML / CFT Policy

Version 3.5

AL DHAHERY
Money Exchange
Licensed by Central Bank of UAE

Title	**AML/CFT Sanction Policy Procedures**
Department	**Compliance Department**
Information Classification	**Public**
Policy Supported	**Al Dhahery Money Exchange- Compliance Program**
Current Version	**Version 3.5**
Review Cycle	**Annually**
Due Date for Review	**August 2024**

Document Contact Details

Role	**Designation**
Author	**Ahmed Mohamed Awes**
Reviewed by	**Compliance Committee**
Approved by	**Owner**

Document Distribution List

SI Number	**Designation**
1	**All Employees**
2	**Correspondent Banks/ Business Partners**

Policy Version Control Record – Revision History

Version	Policy Name	Revision Date	Reason For Implementation	Next Scheduled Review Date
1.0	**AML / CFT Policy Procedures**	**May 2019**	**AML/CFT Sanction policy**	**2019**
2.0	**AML / CFT Sanction Policy Procedures**	**November 2019**	**Revision of AML/CFT Sanction policy**	**2020**
2.1	**AML / CFT Sanction Policy Procedures**	**June 2020**	**Revision of AML/CFT Sanction policy**	**October 2020**
2.2	**AML / CFT Sanction Policy Procedures**	**November 2020**	**Revision of AML/CFT Sanction policy**	**November 2020**
2.3	**AML / CFT Sanction**	**December 2020**	**Revision of AML/CFT Sanction policy**	**November 2021**

	Policy Procedures			
3.0	**AML/CFT Policy**	**September 2021**	**Revision of AML / CFT Sanction Policy Procedures**	**November 2022 or as per changes implicated by CBUAE**
3.1	**AML/CFT Policy**	**December 2021**	**Amended Chapter 16 of the standards for the regulations regarding Licensing and Monitoring of Exchange Business**	**December 2022 or as per changes implicated by CBUAE**
3.2	**AML/CFT Policy**	**April 2022**	**Added DNFBPs, DPMS and International Bodies**	**April 2023 or if needed**
3.2	**AML/CFT Policy**	**September 2022**	**Amended STR/SAR Process as per Notice 3324.2022 STR Guidance for EHs**	**April 2023 or if needed**
3.3	**AML/CFT Policy**	**April 2023**	**Amended EDD 16.11 of the standard. Amended TMS rule of cancelation related to compliance. Internal List Management. Aggregate score. RRS Reporting Documentation.**	**April 2024 or if needed**
3.4	**TF/PF Inclusion**	**August 2023**	**Added TF/PF Section as per Notice 2196.2023 Thematic Review on TFS**	**August 2024 or if needed**
	Post STR/SAR	**August 2023**	**Added post STR/SAR Section as per Notice 2197.2023 Guidance for EHs**	**August 2024 or if needed**
	Financial Illegal Organizations	**August 2023**	**Added Financial Illegal Organizations Section as per Notice 3599.2023 Guidance on Latest AML/CFT Guidelines and Illegal Organizations**	**August 2024 or if needed**
	Occasional Transactions	**August 2023**	**Added Occasional Transactions Section as per Notice 3599.2023 Guidance on Latest AML/CFT Guidelines and Illegal Organizations**	**August 2024 or if needed**
	Requirements for Correspondent relationships	**August 2023**	**Added Requirements for Correspondent relationships as per Notice 3599.2023 Guidance on Latest AML/CFT Guidelines and Illegal Organizations**	**August 2024 or if needed**
	Ongoing Monitoring of Business Relationships	**August 2023**	**Added Ongoing Monitoring of Business Relationships as per Notice 3599.2023 Guidance on Latest AML/CFT Guidelines and Illegal Organizations**	**August 2024 or if needed**
	Additional Correspondent Banks for Remittance	**August 2023**	**As per Approved NOC from CBUAE**	**August 2024 or if needed**

3.5	**Customer Risk Assessment Methodology**	**October 2023**	**Blacklist Percentage match was considered as additional parameter in Onboarding Risk Scoring.**	**October 2024 or if needed**
	Typology and Red Flags Indicator	**October 2023**	**Typology and Red Flags Indicator updates as per the latest guidelines**	**October 2024 or if needed**
	Rules	**October 2023**	**Addition of New Rules.**	**October 2024 or if needed**

Policy Approval

The undersigned acknowledged that they have reviewed the Al Dhahery Money Exchange AML/CFT Policy and they agree with the approach it presents. Any further changes to this Policy in future can only be recommended by the Risk Officer/BCO, Alternate Compliance Officer (ACO) and Compliance Officer and can only be approved by the Owner.

Name and Title		**Signature**
Prepared By:	**ACO** **Umair Abbasi**	
Reviewed By:	**Chief Compliance Officer CCO:** **Ahmed Mohamed Awes**	
Approved By:	**Owner:** **Samira Khamis Mahdi Saeed Alblooshi**	

Contents

Executive Summary

Money Laundering now has become a Global concern and is the mother of all crimes. The fight against money laundering is an evolving and continuous process. Money laundering not only harms the public as a whole but it shakes the financial services industry. It is clearly in the best interest of the financial industry to take appropriate actions to prevent money laundering. The United Arab Emirates recently strengthened its legal framework to fight money laundering and terrorist financing but, as a major global financial center and trading hub, it must take urgent action to effectively stop the criminal financial flows that it attracts. In the past few years, the UAE has made significant improvements to its AML/CFT system including developing the National Risk Assessment (NRA), addressing technical deficiencies in legislation and regulation, strengthening co-ordination mechanisms across the Emirates, strengthening the Financial Intelligence Unit (FIU) and assigning supervisors for previously non-covered sectors.

The UAE understands the risks it faces from money laundering, terrorist financing and funding of weapons of mass destruction is still emerging, following recent national risk assessment. The risks are significant, and result from the UAE's extensive financial, economic, corporate and trade activities, including as a global leader in oil, diamond and gold exports. The UAE's strategic geographical location between continents, in proximity to conflict zones and its own jurisdictional complexity of 7 Emirates, 2 financial free zones and 29 commercial free zones further increase the UAE's risk of attracting funds with links to crime and terror.

ADME has demonstrated a high-level commitment to better understand and mitigate its money laundering/terrorist financing (ML/TF) risk in a coordinated way and has an emerging understanding of its ML/TF risks. The AML/CFT policies & procedures are a good starting point for expressing ML/TF threats and vulnerabilities at ADME. The Compliance Committee has begun implementing a comprehensive AML Strategy to strengthen the overall AML/CFT framework of ADME.

This document is based on FATF 40 Recommendations and lays down the Anti Money Laundering Policies and Procedures to be strictly adhered by personnel working in each functional area. These guidelines have been framed to ensure effective practices are implemented to counter the problem of Money Laundering and that ADME is not made the victim of any Financial Crime. It is ADMEs endeavor for strict compliance in letter and spirit to the regulations under AML Law and the requirements as per the U.A.E. regulators of AML namely Central Bank of the UAE and regulations stipulated by our global partners.

Introduction

Purpose

The purpose of this document is to set out in detail the policies to be followed by the Licensed Person "Al DHAHERY Money Exchange" under the CBUAE Standards of the Regulations Regarding Licensing and Monitoring of Exchange Business ('the Standards'). The policy applies to all our branches, offices and management office in the UAE. It will create awareness among all staff members and Department Heads about Money Laundering/Terrorist Financing and the ways and means of combating the same effectively and to ensure that company and its staff will not knowingly assist criminals to launder proceeds of drug sales, terrorism or other serious crimes.

Scope

The scope of this document is to combat any act of money laundering and establish effective controls within the organization to ensure that the company restrains itself from being made a vehicle for Money laundering. To implement adequate due diligence on new and existing customers, sound Know-Your-Customer (KYC) norms, continuous training of all relevant staff members and good reporting procedures to safeguard the organization from the dangers of Money Laundering. The scope of permitted activities that the licensed person "ADME "can carry out and to which the present policy applies includes the following:

- **Dealing in the sale and purchase of foreign currencies.**
- **Executing remittance operations.**

Review and Changes

- **Any changes in laws and regulations may also trigger a review of this policy document. The Chief Compliance Officer of ADME is responsible for tracking of all regulatory pronouncements applicable to this policy.**
- **Any changes in the policy will be affected only upon approval by the Board of Directors**

Date of Next Review

ADME will ensure that this policy document is reviewed once in a year and when any new regulations are released by Central Bank of the UAE and/or our global partners.

Policy Statement AML/CFT

The fight against Money Laundering and terrorism financing is a priority for Al Dhahery Money Exchange. We recognize that the fight against Money Laundering and Terrorist Financing is team effort. We support the major International Organizations, which collectively set and enforce standards for Anti-Money Laundering and Counter-Terrorist financing policies and programs such as FATF, UN & Local Regulatory Authorities such as Central Bank of the UAE. ADME senior management is committed to the highest standards of Anti Money Laundering (AML) and Counter Terrorist Financing (CTF) compliance and requires management and employees to adhere to these standards to prevent use of our products and services for money laundering purposes to safeguard the interest of our customers, our staff and the communities.

Scope

The policy must provide for at least the following:

- **Applicability of the policy.**
- **Definitions, stages and techniques of money laundering and terrorism financing.**
- **Overview at a high level of the principles adopted by the company for the prevention of money laundering and terrorist financing, which will include:**
- **Customer identification and verification**
- **Establishment of purpose and nature of business relationship**
- **Sanctions screening**
- **Customer account and transaction monitoring**
- **Correspondent banking relationships**
- **Reporting of suspicious or unusual transactions**
- **Overview of the AML function.**
- **Risk-based methodology.**

- **Staff training.**
- **Record retention.**

Functional Responsibility

Responsibility for ensuring implementation of the policies and procedures laid down in this manual will lie with the Compliance Department. The Chief Compliance Officer of ADME will be the owner and custodian of this manual. The owner takes the ultimate responsibility for maintaining this manual to keep it updated according to changing needs of the organization and in response to changes in applicable regulations.

Standards for AML/CFT

The Policy sets the tone at the top, defines core principles to combat money laundering and terrorist financing activities and provides protection to AL Dhahery Money Exchange LLC ("the Company"), against exploitation by perpetrators. This policy was adopted to achieve compliance with the following regulatory guidelines:

CBUAE OUTREACH EVENT on Financial Crimes Institutional Risk Assessments for LFIs 18/08/2021

AML/CFT guidance for LFI's on STR 06/07/2021

CBUAE AMLCFT Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions 04/07/2021

CABINET DECISION NO 74 Issued on 27/10/2020.

Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions

CBUAE guidelines on AML/CFT Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations Guidelines for Financial Institutions for June 2021

Law No. 1/2004, the Counter Terrorism law

Cabinet Decision No (10) of 2019 concerning the implementing regulation of Decree Law No. (20) Of 2018 on of Anti-Money Laundering & Combating the Financing of Terrorism and Illegal Organizations.

Decree Law No. (20) Of 2018 on Anti- Money Laundering and Combating the Financing of Terrorism and Illegal Organizations

The Standards for the Regulations Regarding Licensing & Monitoring of Exchange Business set Regulatory Authorities by Central Bank 2018

CBUAE Notice No. 3090.2021 Updated Guidelines on Anti- Money Laundering.

CBUAE Notice No. 3091.2021 regarding Anti- Money Laundering and Combating the Financing of Terrorism & Illegal Organization

AL Dhahery Money Exchange's AML /CFT sanction compliance Program.

Notice No: CBUAE/BSD/N/2021/5271 Amended Chapter 16 of the standards for the regulations regarding Licensing and Monitoring of Exchange Business and AMLCFT Guidance for Licensed Exchange House.

Notice No. 1381/2022 re Clarifications on Updated Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations 28/03/2022

Notice No. 1163/2022 re Sectoral Report - Money Laundering and Terrorism Financing Risk Assessment 16/03/2022

Notice No. 3354.2022 re Clarifications on Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting 16/08/2022.

Notice No. 3157.2022 re Guidance for Licensed Financial Institutions on the Risks relating to Politically Exposed Persons 02/08/2022.

User of the AML/CFT Sanctions Policy

This AML / CFT Policy is for use of all Employees, management and other stakeholders including regulator, customers, counterparties and correspondent banks etc.

Custodian of the AML/CFT Sanctions Policy

This document is owned by the Compliance Department of the Company and is in custody of the Compliance Officer and Alternate Compliance Officer of the Company. This Manual shall be published internally for the staff of AL Dhahery Money Exchange. AL Dhahery Money Exchange's AML/CFT Compliance Program, policy and procedures are reviewed and approved by the owner, Manager-in-Charge and Compliance Officer. The Compliance function is an independent function headed by Compliance Officer which directly reports to the Owner. AL Dhahery Money Exchange has established a Compliance Committee to oversee key operational decisions for Compliance.

Key Definitions

Money Laundering

The conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions.

Stages in Money Laundering:

Placement

Placement is the initial transformation of illicit cash into other assets. At this stage, the source of the cash is still obvious, so money launderers exploit weak AML controls, use deception, or use unknowing, complicit, or corrupt parties to place their cash

Layering

This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds.

Integration

Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions

Terrorist Financing

Terrorist financing refers to the providing or facilitating funds to sponsor terrorist activity. It may involve funds raised from legitimate or illegitimate sources such as personal donations, profits from the businesses and charitable organizations as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. This is one of the major threats faced by all financial institutions globally.

Economic Sanctions

Economic sanctions may include various forms of trade barriers, tariffs, and restrictions on financial transactions. Economic sanctions generally aim to change the behavior of elites in the target country.

Beneficial Owner

Beneficial owner means the 'Natural Person' who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a juridical person. A Natural Person who owns 5% or above of the juridical person is treated as an UBO.

Correspondent banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world.

Central Bank of the UAE

Central Bank of the United Arab Emirates is the state institution responsible for managing the currency, monetary policy and banking regulation in the United Arab Emirates (UAE).

Shell Bank

Shell banks are financial institutions that do not maintain a physical presence in any country. AL Dhahery Money Exchange is prohibited from entering into a correspondent banking relationship with shell banks.

Foreign Politically Exposed Person and Politically Exposed Person (FPEP/PEP)

FPEP means an individual who is or was previously entrusted with a prominent public function by a foreign country such as heads of state or government, senior politicians, senior government officials and judicial or military officials, senior executives of state-owned corporations, senior officials of political parties, Head of an International Organization (HIO), and such individual's family members or close associates.

PEP means an individual who is or was previously entrusted with a prominent public function by a local country such as heads of state or government, senior politicians, senior government officials and judicial or military officials, senior executives of state-owned corporations, senior officials of political parties, Head of an International Organization (HIO), and such individual's family members or close associates.

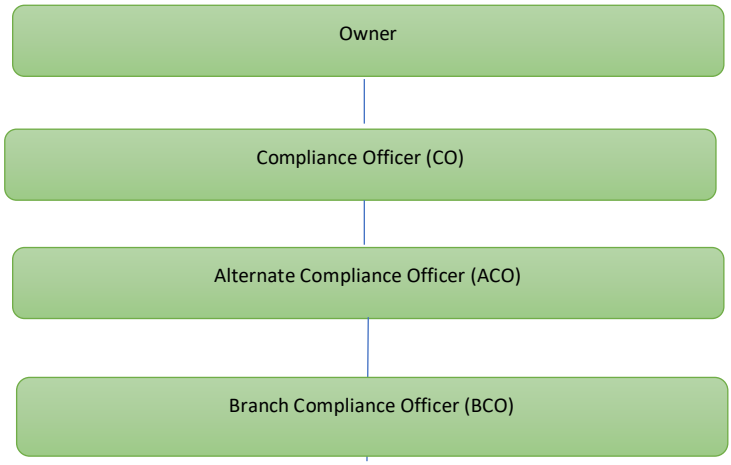
Foreign PEPs & Domestic PEPs EDD:

Conducting suitable risk management systems, prior approval establishing a business relationship, establish the source of funds (SOF), source of wealth (SOW) and enhanced ongoing monitoring over such relationship.

Management and Corporate Governance

Corporate governance broadly refers to mechanisms and processes by which the ADME is managed, controlled and directed. Governance structures and principles identify the distribution of powers and responsibilities within the management structure of an ADME.

Compliance Organization Chart



Key Roles and Responsibilities

Owner-Responsibilities

- **The organization structure of ADME Compliance Department is approved by its Owner and therefore it must reflect the independence reporting line of the compliance which directly reports to the Owner.**
- **The Owner is responsible for the effective management of all aspects/activities related to ADME and therefore of the effectiveness of the AML/CFT procedures implemented and followed by employees.**
- **The Owner of ADME has the ultimate responsibility towards defining a system that ensure the organization performs its duty with due care, that comply with applicable laws, regulations and sanctions obligations as well as satisfy the needs of their key stakeholders.**
- **It's defined and supervises the implementation of an overall strategy that combines these different elements as well as other stakeholders' objectives.**
- **The Owner shall review and approve the AML/CFT policies & procedures whenever material changes are performed and as a minimum on annual basis.**

General Manager (GM)- Responsibilities

- **The GM must ensure that the policy is continuously updated**
- **It's must ensure that a robust compliance function is established and maintained which supplied with sufficient and adequate tools, capital and human resources are provided to the compliance officer consequently he performs his duty in due care.**
- **The GM must evaluate the effectiveness of the compliance function and compliance officer at the end of each year.**

- **Arrange internal & External independent testing for the compliance function & assure that the gaps identified in the compliance regime are remediated in a timely fashion.**
- **The GM must actively involve in the supervision and implementation of the rules, P&Ps related to AML.CFT and sanctions.**
- **The GM is responsible for the effective management of all aspects/activities related to SE and therefore of the effectiveness of the AML/CFT procedures implemented and follow by employees.**
- **The GM shall also review the AML/CFT policy whenever material changes are performed and as a minimum annually during the first quarter compliance committee meeting.**

Compliance Officer Appointment

According Paragraph 16.4 ADME has appointed Compliance officer who given the specific responsibility of managing its AML/CFT compliance function. The Compliance Officer will directly report to Owner in the company and is part of the Senior Management.

Prior Approval for Appointment – Request for prior approval or NOC letter will be submitted for appointing a Compliance Officer is to be obtained as per Paragraph 16.4.8 of the standard by submitting the following documents to the Banking Supervision Department via email to smp@cbuae.gov.ae (with copy to info.ehs@cbuae.gov.ae and amlcft@cbuae.gov.ae).
ADME is also undertaking and confirming the binding commitment of the Compliance Officer to comply with Paragraphs 16.4.5, 16.4.6 and 16.4.7 of the Standard.

Compliance Officer – Responsibilities

- **Implementing the AML/CFT Sanction compliance program for ADME and ensuring compliance with AML/CFT Sanction Laws, Regulations, Notices, the Standards, and international laws**
- **Making sure ADME is prepared with appropriate AML/CFT Sanction policies, procedures, processes, and controls.**
- **Compliance of the business against internal AML/CFT Sanction policies and procedures in day-to-day activities is implemented**
- **Coordination with the Central Bank and any other competent authorities for any matters regarding AML/CFT Sanction related matters/ queries**
- **Assess all suspicious transaction alerts from employees and take appropriate decisions to report all suspicious cases to the FIU**
- **Transaction Monitoring to identify high-risk, unusual, and suspicious customers/transactions**
- **Submission of Suspicious Transaction Reports to the FIU in timely manner.**
- **Provide support and assistance to FIU with all information it requires for fulfilling their obligations**
- **Regular training for newly hired employees and other staff members, particularly when any state or federal laws change.**
- **Designing the compliance training which covers all persecutes of training schedule including training calendar, fit and proper assessments, handling of noncompliance staff etc.**
- **Necessary reports to the owner on all AML/CFT Sanction issues on a monthly basis**
- **Retention of all necessary supporting documents for transactions, KYC, transaction monitoring, suspicious transaction reporting and AML training.**
- **Prepare Bi-Annual Compliance Reports.**
- **Ensure all key documents pertaining to KYC of customers, customer transactions and STR's are retained for the minimum period of 5 years.**
- **Efficient transaction monitoring including pre monitoring and post monitoring**
- **Implementation of the Whistle Blower Policy**
- **Mandatory reporting to CBUAE done according to the Standards of the CBUAE**

- Create gap analysis document on existing AML/CFT Procedures and current Laws, Regulations, Notices and the Standards of the UAE in order to determine the extent of the level of compliance and recommend actions if required.
- Must have sound knowledge of all applicable AML/CFT Laws, Regulations, Notices, the Standards and other relevant international best practices.
- Must not engage in any part time employment or act as a consultant outside ADME
- Must be a resident of the UAE
- Compliance Officer must not have a Conflict of Interest,
- Must go through a fit and proper test with Central Bank of the UAE
- The Alternate Compliance Officer must be available to ensure the continuity of the AML/CFT compliance function during the period when the Compliance Officer's position is vacant.
- Minimum of forty-eight (48) hours external training in AML/CFT compliance every year

Alternate Compliance Officer

According Paragraph 16.5 ADME has appointed Alternate Compliance officer to strengthen the AML/CFT compliance. The Alternate Compliance Officer will directly report to the Compliance Officer or to the Board of Directors (or to the Owner/Partners where there is no Board of Directors) during the absence of the Compliance Officer.

Prior Approval for Appointment – Request for prior approval or NOC letter will be submitted for appointing an Alternate Compliance Officer is to be obtained as per Paragraph 16.5.2 of the standard by submitting the following documents to the Banking Supervision Department via email to smp@cbuae.gov.ae (with copy to info.ehs@cbuae.gov.ae and amlcft@cbuae.gov.ae).

ADME is also undertaking and confirming the binding commitment of the Alternate Compliance Officer to comply with Paragraphs 16.5.1 (a) to (g) of this Chapter of the Standard

Alternate Compliance officer – Responsibilities

- Administration of compliance monitoring, compliance on-boarding functions including KYC and Customer Due Diligence
- Receive Internal Suspicious Transaction Reports (ISTR) from branches
- Investigate, Report and file Suspicious Transaction Report (STR) to CBUAE, if required
- Correctly filing with the CB UAE any periodic reports required by them
- Monitoring and testing of transactions.
- Monitoring trade-based money laundering and tracing structured transactions.
- Investigate, research, and take action for the exceptions for name clearance & monitoring of payment transactions.
- Maintain appropriate records and arrange monitoring of suspicious accounts periodically.
- Provide periodical training to the entire staff of the organization
- Advise the business regarding the AML/CFT aspects in relation to the development of new products services in new and existing markets.
- Provide support and advice to other departments in relation to the application of rules and regulations to their function.
- Monitor the performance of the AML/CFT Compliance Program and related activities on a continuing basis, taking appropriate steps to improve its effectiveness.
- Review and address AML/CFT & Watch list and alerts. Update the blacklists on a regular basis.

- Liaison with the compliance team of the correspondent bankers and satisfactorily answer any

queries posed.

- Coordinate as support regarding all AML/CFT Sanction related matters/ queries from the Central Bank and any other competent authorities in absence of Compliance officer.
- Collaborate with external auditors and HR when needed.
- Implementation and execution of the regulations issued by CBUAE and the organization's AML/CFT policies & procedures.
- Monitoring day-to-day transactions of the branch for any unusual/ suspicious behavioral pattern.
- Performing more extensive, due diligence for high-risk amounts/ countries/ customers and include proactive monitoring for suspicious types of activities.
- Educating the staff in the branches regarding AML/CFT 'know your customer's procedures.
- Maintaining records as required by ADME AML/CFT Sanctions policy & procedures.
- Must not engage in any part time employment or act as a consultant outside ADME.
- Must be a resident of the UAE
- Reporting of the Alternate Compliance Officer will be to the Compliance Officer
- Must go through a fit and proper test with Central Bank of the UAE
- The Alternate Compliance Officer must be available to ensure the continuity of the AML/CFT compliance function during the period when the Compliance Officer's position is vacant.
- Minimum of forty-eight (48) hours external training in AML/CFT compliance every year.
- Participation in the Compliance Committee meeting and assisting the Compliance Officer in the responsibilities of the Compliance Committee Meetings.

Branch MLRO – Responsibilities

- Responsible to carrying out the Branch compliance officer function of the organization to ensure the day today functions are adhering to the CBUAE/UAE regulations.
- Act as a liaison between the Head Office Compliance wing and Branches regarding Compliance matters, queries emails and investigations
- Monitoring day-to-day transactions of the branch for any unusual, structured, suspicious and blacklisted ones
- Educating the staffs in the Branches regarding Anti-Money Laundering & Combating Terrorist Financing and 'Know Your Customer' procedures
- Record keeping as required by the Exchange AML/CFT Policy & Procedures
- To take proper remedial actions and inform Compliance Officer if violations are identified
- Provide guidance on how to identify suspicious activities and structured transactions
- Advise branch staff of proposed regulatory changes and provide in-house training to branch staff
- Reporting of unusual or suspicious transaction to Chief Compliance Officer
- Implementation of the Regulations issued by the Exchange and our Anti-Money Laundering and Combating Terrorist Financing Policy and Procedures across Branches
- Performing more extensive due-diligence for high-risk amounts, countries, customers and include proactive monitoring for suspicious activities
- Willing to take on extra responsibility relating to AML /CFT & Compliance matters and to bring in ideas and suggestions for process improvement
- Strictly follow the company's policy and procedure without fail
- Reporting to Compliance Officer/Alternate Compliance officer
- Approval of transactions as and when required

Resignation & Appointment of the Compliance Officer and Alternate Compliance Officer

ADME will notify the Banking Supervision Department and the AML/CFT Supervision Department, within five (5) working days of the date of resignation, of the Compliance Officer or Alternate Compliance Officer the date upon which the position becomes vacant in any other manner with reasons thereof via email respectively to info.ehs@cbuae.gov.ae and amlcft@cbuae.gov.ae;

Compliance Officer & Alternate Compliance Officer: In ADME, we understand the relevance of a Compliance Officer and therefore according to the Central Bank rules as per the Paragraphs 16.4 and 16.5 in the Standard

ADME - will propose a permanent replacement, within a period of ninety (90) calendar days from the date when the position of the Compliance Officer falls vacant, by submitting a request of No Objection to the Banking Supervision Department as per Paragraph 16.4.8 and 16.5.2 of the Standard also Alternate Compliance Officer must be available to ensure the continuity of the AML/CFT compliance function during the period when the Compliance Officer's position is vacant.

Compliance Committee

ADME has an AML/CFT Committee which comprises of the key officials of the organization and is headed by the Owner (Chairman of the committee).

The Committee shall have the authority to undertake the specific duties and responsibilities described below and the authority to undertake such other duties as are assigned by law. The Committee shall be composed of at least four (4) members

The Compliance Committee will include the following members at a minimum:

- **The Owner**
- **Manager-In-Charge**
- **Compliance Officer (CO)**
- **Alternate Compliance Officer (ALCO)**
- **Manager Operations**

Meetings and Procedures

a. **The Committee will hold at least four (4) regularly scheduled meetings each year.**
b. **The Committee shall maintain written minutes or other records of its meetings and activities. Minutes of each meeting of the Committee shall be distributed to each member of the Committee.**
c. **The Owner, Manager-In-Charge, Compliance Officer, Alternate Compliance Officer and Internal Auditor will meet at least once in six (6) months to discuss all aspects of the business and the minutes of above meetings would be available for the verification of the Auditors or Central Bank Examiner, in case of unavoidable circumstances.**

Responsibilities

Oversee the Company's compliance programs, including review of, with the appropriate members of management, the organizational structure, staffing, implementation and management's assessment of the

effectiveness of the Company's compliance programs relating to the Company's principal legal and regulatory compliance risks, the related policies and procedures, and the adequacy of the resources for those programs. Review of the Company's compliance policies and procedures shall include the Company's Code of Conduct, education and training, and other written compliance policies and procedures that guide the Company and the conduct of its agents in day-to-day operations.
Recommend the name(s) of appropriate External Auditors for the approval of the Owner to perform an Agreed-Upon Procedures on the AML/CFT Sanction compliance function annually.

- **Review risk identification, assessment and mitigation plans**
- **Periodically review resources, systems to ensure that they are appropriate to the nature, size and complexity of the business.**
- **Review recommendations from the Annual Report of the Compliance officer.**
- **Review findings of internal audit, independent review of the AML/CFT Sanction compliance function by External Auditors, the Central Bank examinations and all related action plans.**
- **Necessary modifications to the Compliance Program.**
- **The Compliance Officer will update to the Committee any data suggesting significant non-compliance that could affect the Compliance Program or the Company. Any data suggesting significant non-compliance involving any of the Company's officers shall be reported to the committee immediately.**
- **Review regulatory compliance risks**
- **Review significant risk exposures or compliance violations and the steps that have been taken to monitor, correct and/or mitigate such violations or risks.**

Audit Committee Meeting

ADME has an AML/CFT Audit Committee which comprises of the key officials of the organization and is headed by the Owner (Chairman of the committee).

Purpose

The Audit Committee shall have the authority to recommend the names of the appropriate External Auditors for the approval of the owner (Chairman of the committee) to carry out the annual financial audit.

Membership

The Audit Committee will include at least four (4) members at a minimum:

- **The Owner**
- **Manager-In-Charge**
- **Internal Auditor**
- **Compliance Officer**

Meetings and Procedures

a. The Audit Committee will hold at least four (4) regularly scheduled meetings each year.
b. The Audit Committee shall maintain written agenda and minutes or other records of its meetings and activities. Minutes of each meeting of the Committee shall be distributed to each member of the Committee for their acknowledgement.

Responsibilities

- **The Audit Committee meetings will hold quarterly meetings to review the Internal Audit finding and implement corrective measures.**
- **The Audit Committee will also recommend the name of appropriate External Auditors for the approval of the Owner to carry out the Annual Financial Audit for next subsequent year.**
- **The Audit Committee will review and ensure that the Internal Audit Charter and the Internal Audit Plan and obtain approval from the Owner.**

- **The Audit Committee will also review all internal/external audit reports, management letters, etc. on periodic basis to ensure that the audit function is performed at the exchange as per the requirements.**
- **The Audit Committee will review the gaps identified and recommendations made by the Internal Auditor in their monthly and quarterly reports and shall ensure its implementations.**

Products and Services

Products & services are the integral part of ADME marketing & business development. A product is a tangible item that is put on the market for acquisition, attention, or consumption, while a service is an intangible item, which arises from the output of one or more individuals. Although it seems like the main distinction between the two concepts is founded on their tangibility, which is not always the case. In most cases, services are intangible, but products are not always tangible. ADME has wide range of products & services to serve the purpose of customer satisfaction.

Remittances –Money Transfers

Remittances are transfer of money from one jurisdiction to another on behalf of its customers, whether natural persons or juridical persons, who are physically present in the UAE. ADME has following money transfer services to its customers for both home remittance and Trade Based Transaction.

convera **Make smart money moves - Western Union Business Solutions (Convera Malta Financial (Malta) Limited) is located in Birkirkara, Malta and is part of the Activities Related to Credit Intermediation Industry.**

Western Union Business Solutions was formed in 2009, when Western Union acquired Custom House, an award-winning industry leader with over 18 years of experience in international payments and currency risk management. Following the acquisition of Travelex Global Business Payments in 2011, the company has expanded to become one of the world's leading non-bank providers of cross-border business payments.

NIUM **Nium's origins lies in InstaRem, co-founded in 2014 by Prajit and Michael Bermingham. The driving force behind the company was Prajit's own frustrating experience with cross-border remittance payments, and his desire to simplify the process for businesses and consumers alike. InstaRem quickly won customers across the globe thanks to its intuitive user experience, competitive rates, and broad reach. Core to the success of the InstaRem service is an advanced global payments platform - a platform built for simplicity, scale and speed.**

INSTANT CASH GLOBAL MONEY TRANSFER **INSTANT CASH GLOBAL MONEY TRANSFER (popularly known as INSTANT CASH) is one of the fastest growing money transfer companies in the world. Head Office in the UAE is supported by local offices in the Qatar, Oman, Bahrain, India, Pakistan, Bangladesh and Philippines. With a Network of 250,000 locations across the globe**

Founded in 1851, Bank of the Philippine Islands is the first bank in the Philippines and in the Southeast Asian region. BPI is a universal bank and together with its subsidiaries and affiliates, it offers a wide range of financial products and solutions that serve both retail and corporate clients.

Kotak Mahindra Finance Ltd. in 1985 to becoming one of the country's most trusted financial institutions today, ADME use it for home remittances for Indian customers.

United Bank Limited is a Pakistani multinational commercial bank which is based in Karachi, Pakistan. It is one of the largest banks in the Pakistani private sector, with over 1,400+ branches across Pakistan, 19 branches overseas, and a customer base exceeding 4 million

IndusInd Bank is one of India's leading financial services brands. It's the preferred banking solutions provider and partner for approximately 35 million customers across the country, including individuals, large corporations, various government entities and PSUs. It's banking network spans 2606 branches/ Banking outlets and 2875 ATMs spread across India, covering 1,38,000 villages, and it also have representative offices in London, Dubai, and Abu Dhabi. The Bank offers a wide range of products and services for individuals and corporates, including microfinance, personal loans, personal and commercial vehicle loans, credit cards and SME loans.

Mutual Trust Bank Ltd. (MTB) is a third-generation private commercial bank, based in Dhaka, Bangladesh and has been adjudged as the Best Financial Institution of 2014 at the DHL-Daily Star Business Awards 2015. Earlier, MTB had also received the first-ever best "SME Bank of the Year" and best "Women Entrepreneurs' Friendly Bank of the Year" by Bangladesh Bank and SME Foundation. MTB has recently been awarded the Best Presented Annual Report-2018 (3rd position) in the Private Banks category by The Institute of Chartered Accountants of Bangladesh (ICAB). MTB aspires to be one of the most admired banks in the nation and recognized as an innovative and client-focused company. With our current network of 119 branches & 33 Sub branches, 200 Agent Banking Centers, 18

kiosks, 310 modern ATMs including 6 CRM Booths, 4 Air Lounges, over 3,220 Point of Sales (POS) machines, located in prime commercial, urban and rural areas, MTB offers fully integrated real time Online Banking Services, Internet and SMS Banking to its clientele, through a dedicated Team of experienced Relationship Managers and Alternate Delivery Channels (ADC)."

African Banking Corporation (ABC) Bank Limited is a financial services institution with 38 years' experience that is licensed and regulated by the Central Bank of Kenya. The Bank operate across the country through 11 branches, working with over 55,000 customers to make them ACHIEVE THE EXTRAORDINARY.

ABC Bank Limited provides reliable and efficient services including banking, stock brokerage, investment advisory, insurance, risk management and financial services. Regionally, ABC Bank Limited operates in Uganda through our subsidiaries ABC Uganda and ABC Capital.

Foreign Exchange Transactions

ADME deals in all major currencies and provides its customers foreign exchange services at its branches operating in the United Arab Emirates.

Client Acceptance Policy

ADME shall follow customer acceptance policy and procedures, in accordance with national and international regulations and best practices, to prevent the commencement of business relationships with customers against whom sanctions or restrictions have been imposed, or with customers who pose a non-acceptable level of risk to the company and its business operations. ADME will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate. ADME shall establish AML/CFT procedures to assist and guide employees in carrying out their responsibilities and ensure that ML/FT risks are taken into consideration in the company's daily operations. These procedures should be read in conjunction with UAE laws and the CBUAE regulations. The Following is a list of Procedures, which should be strictly followed:

Identification and Verification of Client Identity

ADME will establish the identity of its clients and beneficial owners prior to establishing business relationships with such persons. Identity is generally established by obtaining the name, date of birth (in the case of individuals), address and such further information that may be required by the Regulatory authority and laws of the relevant jurisdictions.

Verification of Identity

ADME will take reasonable measures to verify identity when establishing a business relationship as noted below, subject to applicable CBUAE requirements.

Natural persons: identity will be verified to the bank's satisfaction on the basis of official identity papers or other reliable, independent source documents, data, or information as may be appropriate under the circumstances.

Corporations, partnerships: **identity will be verified on the basis of documentary evidence of due organization and existence.**
Identification documents, if used for verification purposes, must be current at the time of opening and copies of such documents will be obtained.

Beneficial Owner

Beneficial ownership, for AML purposes, must be established for all accounts. Beneficial owners will ordinarily include the individual

- **Who generally have ultimate control through ownership or other means over the funds in the account and/or?**
- **Who is the ultimate source of funds for the account and whose source of wealth should be subject to due diligence?**

Mere signature authority does not necessarily constitute control for these purposes. The meaning of beneficial ownership for purposes of determining who should be subject to due diligence is dependent on the circumstances and due diligence must be done on all beneficial owners identified in applying the following principles:
Natural persons: **when the account is in the name of an individual, FLA must establish whether the client is acting on his/her own behalf. If doubt exists, the bank will establish the capacity in which and on whose behalf the accountholder is acting.**

Legal entities: **where the client is a business entity, the BCO will understand the structure of the company sufficiently to determine the provider of funds, the beneficial owner(s) of the assets held by the company and those with the power to give direction to the directors of the company. This principle applies regardless of whether the share capital is in registered or bearer form.**

Partnerships: **where the client is a partnership, the BCO will understand the structure of the partnership sufficiently to determine the provider of funds and the general partners.**

In each of the above cases, the FLA/BCO will make a reasonable judgment as to the need for further due diligence. The identity of each beneficial owner will be established and, as appropriate, verified unless the identity is previously verified in accordance with the beneficial owner's role as a client. Identity will be verified to the bank's satisfaction on the basis of official identity papers or other reliable, independent source documents, data, or information as may be appropriate under the circumstances. In the event verification is based on identity papers, copies of such identity papers should be obtained.

Ultimate Beneficial Owner

The UAE Federal Decree Law 20 of 2018 on Anti Money Laundering and Countering the Financing of Terrorism (the "AML Law") and the Cabinet Decision 10 of 2019 issued under the AML Law require identifying the ultimate individual beneficial Owner(s) of businesses registered in the United Arab Emirates. An Ultimate Beneficial Owner is an individual who ultimately owns or controls 25% or more of a Business Partner, whether directly as a shareholder or indirectly via control of companies, other entities or structures that controls the Business Partner (the "UBO").
The identity of each beneficial owner will be established and, as appropriate, verified unless the identity is previously verified in accordance with the beneficial owner's role as a client. Identity will be verified to the bank's satisfaction on the basis of official identity papers or other reliable, independent source documents, data, or information as may be under the circumstances. In the event verification is based on identity papers, copies of such identity papers should be obtained.

Powers of Attorney/Authorized Signatories

The relationship between the holder of a power of attorney or another authorized signatory, the accountholder and if different, the beneficial owner of the account, must be understood. The identity of a holder of general powers over an account (such as the power to act as a signatory for the account) will be established and, as appropriate, verified.

Walk-In Customers

ADME shall specifically address measures to satisfactorily establish and verify the identity of Walk-In customers. The threshold limit set for walk-in customer is below AED 3500 for foreign Currency transactions. ADME shall apply the CID process in accordance with Paragraph 16.8 for a person who repeatedly exchanges FC (F example once a week) of value below AED 3,500 per transaction.

Customer Due Diligence

Using a risk-based approach, the FLA must ensure that it collects and records a sufficient amount of pertinent information when establishing a business relationship and must update the client profile with additional information as the relationship develops. The information should enable an independent reviewer (whether internal or external) to understand the client and the relationship on the basis of the information recorded. In the event the client is not the beneficial owner, not all of the information contemplated by this policy will be obtained with respect to the client; however, in these circumstances, the relevant information will be obtained with respect to the beneficial owner(s). The criteria to be taken into account for evaluating the risk of accepting customers may comprise:

- **Inclusion in sanction lists**
- **Country of origin or residence or business activity**
- **Customer profession or business activity**
- **Source of income and wealth**
- **Origin of funds**
- **Type of products, services and channels that the customer intends to use**
- **Expected type, volume and frequency of transactions**
- **The legal status of the company (legal entities)**

PEP -CLIENT ACCEPTANCE POLICY

The regulatory approach to dealing with PEPs predates the establishment of the RBA. Now that the RBA has been enshrined as the first of the FATF Recommendations and in the interests of increased effectiveness, the ADME believes that it is acceptable for PEPs to be integrated into an overall RBA and thereby be subjected to a more tailored and risk-based control framework. A basic element of the PEP definition is that a PEP is a natural person. The involvement of a PEP in the management of an entity-based relationship, as treated below, could increase the risks involved in establishing or maintaining a relationship with such an entity, but may not necessitate the categorization of the entity as a PEP. However, accounts for trusts, personal investment companies, foundations, operating companies or other entity-based accounts should, if established for the specific benefit of a PEP, Close Family Member or Close Associate, be subjected to the control framework appropriate for PEPs. Regardless of the approach, ADME would reiterate the key notions that it deems essential to the appropriate management of PEP Risk: The definition also includes the following:

- **The definition of a PEP should focus on those in senior, prominent political positions, who have substantial authority over policy, operations or the use or allocation of government-owned resources and are therefore more vulnerable to grand corruption**
- **The definition of a PEP should not be diluted by the inclusion of categories of natural persons who may exert considerable influence and are politically connected, but do not hold public office**

- **While, under certain circumstances, relatives and close associates should be subjected to the same control framework as PEPs, they should not themselves be considered PEPs in all cases**
- **The principle of "once a PEP, always a PEP" runs counter to an appropriate RBA and should be considered very carefully before being applied**
- **Regulatory requirements set out the need for reasonable risk-based measures for identifying PEPs, it is noted that while this may include automated screening, this is not necessary in all circumstances**

PEPs are also often the subject of intense public and media scrutiny; with the increased possibility of commensurate reputation risks for maintain relationships with them. This guidance considers the financial crime risk of a PEP and not the reputational risk which ADME should clearly consider, in line with their risk appetite. PEP client acceptance policy refers to the procedures & guidelines involved during on boarding of a Politically Exposed Person. It includes below procedures of PEP Risk Management Framework

Senior Management Approval

Both the Manager in Charge and the Chief Compliance Officer must approve the business relationship with legal entities. Where an Ultimate Beneficial Owner is PEP, the business relationship with such legal entity must be established only after obtaining approval from the Board of Directors.

Enhanced Monitoring (manual or automated)

Accounts with a PEP relationship should, using an RBA, be subject to proportionate enhanced monitoring to detect unusual and potentially suspicious activity.

***PEPs will be subject to EDD measures, and discreet inquiries must be made for ascertaining the purpose and ultimate beneficial owner for each and every transaction made by them. In case of any suspicion, then an STR has to be escalated in GoAML System.**

PEP Declassification

There is no agreed method for determining the time period that an individual should be regarded as a PEP after they have left the public function that gave rise to the initial categorization. The risk associated with PEP is closely related to the political situation and the inherent corruption risk in their country of political exposure, the office or function they held and the influence associated with that post. Although that influence may substantially reduce as soon as they have left office, a PEP may have been in a position to acquire his or her wealth illicitly, so that a high level of scrutiny with regard to such individuals may be warranted even after they have left office. ADME does not believe that the approach known as "once a PEP, always a PEP" is consistent with an RBA to managing financial crime risk. While there will be certain higher risk PEPs were maintaining classification as a PEP indefinitely will be warranted, for other categories, a holistic approach should be taken when considering when a PEP should be de-classified. Where a PEP is deceased but was the source of funds/wealth for close family members' or close associates', a risk-based assessment will need to be made to determine whether those relationships still merit appropriate levels of EDD on their own merits or whether they should be declassified. Any declassification of PEP should be subject to an appropriate level of senior management review and approval. This review should be documented. Once a PEP has been de-classified, their prior PEP status should be noted for investigatory purposes (e.g., in the event of a suspicious activity reporting).

Know Your Customer

The Know Your Customer (KYC) principle constitutes the basis of the AML/CFT framework and is the key to effective protection of financial institutions against financial crime. Knowing your customer before executing transactions is the foremost tool of AML/CFT policies and procedures and involves making all reasonable efforts to determine the true identity of customers and the beneficial ownership

of accounts and ensuring, to the extent possible, that the funds involved in the transactions are originating from legitimate sources and being used for legitimate purposes. The KYC principle comprises the following elements, which complement one another:

The KYC principle comprises the following elements, which complement one another:

- **Customer acceptance (e.g., verifying that the customer is not on sanctions or restrictions lists issued by the competent authorities)**
- **Customer identification and verification**
- **Customer business information**
- **Customer transaction profile**
- **Customer and Enhanced Due Diligence measures according to the customer risk rating.**
- **Continuous monitoring of accounts and transactions (e.g., against the customer's recorded profile and his transaction history)**
- **Assessment of the customer's overall profile**
- **Detection, management and reporting of unusual or suspicious transactions**
- **To ensure that at the time of on boarding a customer a unique identification number (UIN) is issued to the customer**

- **ADME shall implement an appropriate KYC process depending on the risks associated with each customer or transaction. ADME should be able to demonstrate to the CBUAE examiners that the KYC process we have put in place is aligned with UAE Central Bank Standards, their AML/CFT risk profile and is proportionate with the ML/FT and related financial crime risks we face. ADME shall review and update KYC details at frequent intervals according to the customer risk classification, to ensure that the customer information and documents are valid and that any changes are recorded on time. Maintaining up-to-date information assists the Licensed Person with its monitoring obligations as it enables to understand whether the transactions being conducted are consistent with the known business of the customer, his profile and his source of income.**

KNOW YOUR CUSTOMER (KYC) PROCESS: **The process was outlined for the same.**

- **Customer Identification Process (CID)**
- **Customer Due Diligence (CDD)**
- **Enhanced Due Diligence (EDD)**

Customer Identification (CID)

(Foreign Exchange)

- **Foreign currency exchange transactions of value between AED 1 and AED 3,500, ADME shall record the following information on the transaction receipt:**
- **Full name**
- **Address, if available**
- **Mobile number**
- **The exchange house must retain the transaction records in the company's records for further reference. Foreign currency exchange transaction of value between AED 3,500 and AED 34,999.75 or cumulative transactions within a week of more than AED 3,500, ADME shall perform the CID process. ADME shall perform CID by means of one of the following original documents, by order of preference as stipulated**

by the CBUAE:

Approved IDs

- **Emirates ID**
- **Passport (with valid visa for the UAE for non-UAE nationals, this can either be a residence or investor visa for long-time residence or a visit or business visa for shorter durations)**
- **GCC national ID for GCC nationals**
- **Seaman pass /ID for foreign currency exchange transaction up to AED 34,999.75 per week and for money transfer up to AED 27,000 per week.**
- **ADME shall not affect transactions for natural persons who do not have a valid visa for the UAE except in the following circumstances:**
    - **The individual is in the grace period upon cancellation or expiry of the visa/visit visa**
    - **The individual has been granted amnesty**

Customer Due Diligence (CDD)

Customer Due diligence (CDD) is applying care before processing a customer transaction or on boarding a customer. It is the process of obtaining additional relevant details of and information about the customer, to ensure that he conducts transactions in line with his personal profile and business activities. CDD assists the exchange house in ensuring that the source of funds and transaction purpose are legitimate and that the transaction is not related to money laundering or terrorist financing.
The CDD process detailed below must be performed prior to effecting the following transactions:

- **Money transfers, inward or outward: AED 1 – AED 54,999.75**
- **Foreign currency exchange transactions, either one-off or multiple in (90) calendar days: AED 35,000 – AED 54,999.75**
- **Customer (Natural/Legal Entity) -Dual Nationality**
  ADME shall apply special measure while registering customers holding dual nationalities. Such registrations will be subject to compliance team review and approval.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is a measure applied by financial institutions to know more about the customer and his business activities The objective of EDD is to manage and mitigate cases of increased risk. Hence it is not required in all circumstances; it is applied when the customer, requested product or service are considered to be of greater risk, and when there is doubt or suspicion with regard to the transactions conducted by the customer.

Guidelines on conducting EDD on natural persons

- **The EDD process must be performed prior to effecting the following transactions:**
- **foreign currency exchange transactions equal to or above AED 55,000 within (90) days.**

- **Money transfers, inward or outward equal to or above 55,000 within (45) days.**
- **ADME shall set lower transaction limits for foreign currency exchange transactions and outward money transfers for visitors and tourists in accordance with its risk assessment.**
- **EDD measures for natural persons include:**

Foreign currency exchange transactions

- **Evidence of source funds such as a bank statement for cash transactions. Complete information of the purpose of the transactions must also be collected. The FLA must collect appropriate evidence for verification of the purpose of transaction if there is any suspicion regarding the information provided by the customer.**
- **Outward money transfer of value equal to or above AED 55,000, either one off or multiple in (45) days- Evidence of source funds such as a bank statement for cash transactions. Complete information of the purpose of the transactions must also be collected. The FLA must collect appropriate evidence for verification of the purpose of transaction if there is any suspicion regarding the information provided by the customer.**
- **Outward money transfer of value equal to or above AED 55,000, either one off or multiple in (45) days- Information of source funds and the purpose of transaction must be collected and recorded. Complete information of the purpose of the transactions must also be collected. The FLA must collect appropriate evidence for verification of the purpose of transaction if there is any suspicion regarding the information provided by the customer.**
- **If the customer brings cash imported into the UAE for foreign currency exchange transactions equal to or above 60,000 AED, the FLA must: Collect original CDF (Customs Declaration Forms) and kept the original if full amount exchanged if partial of the money writes the amount exchanged and put the ADME stamp. For the source of funds (example: bank statements) must be collected for verification in case the customer pays cash. Complete information of the purpose of the transaction must be collected.**
- **Source of Funds for FC Sale Transactions: Evidence for the source of funds (example: bank statements/SOA or Withdrawal Slip) must be collected for verification in case the customer pays cash.**
- **Source of Funds for FC Purchase Transaction: We will require the source of FC currencies such as;**
- **Purchase receipts from us or from other exchange houses.**
- **FC bank withdrawal receipts or FC Bank account Statements.**
- **Letter of undertaking from customer that he is the beneficial owner of these funds and the source of these funds is legitimate.**

Customs Declaration Forms (CDF)

- **If the customer brings cash imported into the UAE for foreign currency exchange transactions or outward money transfers, the FLA at ADME must also request CDF Form from the customer issued at customs boarders of the United Arab Emirates. The guidelines to collect CDF are as follows;**
    - **Passengers travelling from overseas with FC equivalent over AED 60,000 or its equivalent in foreign currencies need to give the declaration.**
    - **Non-Residents carrying FC equivalent over AED 60,000 or its equivalent in foreign currencies need to give declaration.**

- **"All passengers arriving in the country must declare cash or other bearer monetary instruments in their possession in an aggregate amount exceeding AED 60,000 or its equivalent in foreign currencies by filling out the designated declaration form in accordance with the cash declaration regulation in force in the UAE. Passengers under the age of 18 years old shall not be allowed to bring in cash exceeding the aforementioned permissible limit and any excess cash in their possession shall be added to the allowed limit of their parent/guardian should they be accompanied minors.".**

Enhanced Due Diligence on Exchange Houses (Foreign Exchange)

The EDD Process includes:

- **As per the Federal Law No. (10) of 1980 of the Central Bank all exchange houses shall get the approval from the Central Bank before carrying on exchange business with other exchange houses in the United Arab Emirates**
- **EDD should be conducted on the exchange by collecting the relevant documents to ensure their existence. The List of documents include Central Bank License, Trade license, MOA, AOA, POA, Dewa bill, Telephone bill, Tenancy Contract, VAT Certificate, Share Certificate or Ownership structure to identify the ultimate beneficial owners with their country of origin, the AML Questionnaire to check their adherence to the international standards for AML Policy.**
- **Site Visit to the exchange houses by the CCO prior to the establishment of the exchange business.**
- **To ensure that the exchange house is in line with its nature of business and to meet the partners, beneficial owners or key controllers, senior management of the entity and the number of branches they are operating and update the on-boarding booklet of ADME with the relevant information.**
- **Approval from the senior management for the on-boarding of the exchange house.**
- **Identify the beneficial owners, authorized signatories, partners with their ID documents which constitute the Passport, Emirates ID and Visa as well as sanction screening conducted by our compliance team on the exchange house, Beneficial owners, representatives and key controllers.**
- **When the exchange house appoints an authorized representative/dealer, the authorization letter/letter of undertaking should be collected along with the relationship details of the representative with the exchange house on whose behalf he is doing the transactions, date of issue of the authorization letter, identification documents of the representative, the frequency of transactions, the expected annual turnover of the exchange should be recorded in the customer profile.**
- **A confirmation mail from the exchange house to the dealer's department in ADME regarding the transaction should be sent and after the approval from the department the transaction shall be initiated.**
- **Linking of the dealers to the profile of the exchange house on ADME Tool to mitigate the risk of ML/CFT.**
- **Compare the list of dealers registered on the system with the Authorization Letter received and deactivate any user not listed on the letter from the system**
- **Cross verifies and reconfirm the list of Authorized Dealers once in six months by mail with the Exchange House Management.**

Third Party Transactions

ADME maintains its SOP for third party transactions for individuals:

DEFINITION

Third Party transactions out by a person ('representative') on behalf of another natural person. Crafting the particulars of the deal or serve as the means of receiving a payment on behalf of a natural person or entity.

KYC/CDD/EDD

ADME will conduct stringent CDD/EDD measures for these transactions.

Risk Categorization

Such Transactions will be treated as High-Risk Transaction in "Risk Matrix"

Sanction Screening

Sanction Screening will be conducted in live events and post events against mandatory check lists.

Transaction Monitoring System

"ADME" will apply live rule on third party transactions for robust monitoring.

PROCEDURES - Individuals

In order to identify a third-party transaction and accept transaction by one natural person to another, ADME follows the procedure below:

- **Power of Attorney (POA) from the beneficial owner of funds must be produced by the representative to carry out third party transactions. The beneficial owner shall issue an authorization letter, authorizing the representative the carry out transactions of their behalf in absence of a POA. However, the beneficial owner must visit ADME physically and sign such authorization letter which is valid for not more than two (2) years from the date of issue.**
- **Beneficial owners working as domestic helpers (such as house maid, cook, cleaner etc.) who are unable to visit the branch must issue a letter signed by them authorizing the representative to carry out the requisite transactions.**
- **The Authorization letter must refer to the type of transactions (whether currency exchange or money transfer).**
- **Authorization letter must include the beneficiary details in the case of a money transfer transaction.**
- **The signature of the beneficial owner of funds in the letter of authority must be verified against that in the passport or the Emirates ID.**
- **Both representative and the beneficial owner must be UAE resident.**
- **Collect and verify the original identification documents of both the parties.**
- **Record all transactions in the system against the Unique Identification Number of the beneficial owner of funds. However, for beneficial owners working as domestic helpers, all transactions must be recorded in the system against the Unique Identification Number of the representative.**
- **Record Name and ID details of the representative in the system.**
- **The beneficial owner must undergo the CDD & EDD process, whenever applicable.**
- **Sanction/FPEP screening is mandatory against the names of both the parties.**
- **Names of the representative and the beneficial owner must be printed on the transaction receipt.**

- **The total value of transactions, whether foreign currency exchange or inward/outward remittance, shall not exceed AED 24,000 during a rolling three hundred and sixty-five (365) days from the date of the first transaction for each beneficial owner of funds.**
- **Compliance Officer of ADME Exchange closely monitors all such transaction.**

ADME Verdict for De-Risking

ADME has included the below points as the final verdict in Client Exit policy or termination of a client relationship by the occurrence of the following events.

Termination by Law

- **When ADME has receive court order in respect to an existing or registered customer.**
- **Any subject when ADME has to comply with CBUAE, FIU or other equivalent regulatory requests.**
- **When ADME has to act in accordance with the instruction of UAE Police department.**
- **Any other matters to meet the provisions under law.**

Sanction list

- **When the customer is listed in Money Laundering or Terrorism Financing.**
- **When the customer is identified as he/she has involved in severe crime like Human Trafficking, Smuggling, Narcotic dealing, Tax evasion, corruption etc.**
- **The individual/entity is listed in sanction list of CBUAE List, UN, EU, OFAC, or other similar organization.**
- **When the customer is identified as PEP but the final decision of termination is limited to CCO and GM approval.**
- **Any other matters impending under sanction list.**

Others

- **At the event of death or dissolution of either party**
- **When the customer has conducted fraudulent attempt/activities.**
- **The customer has intentionally abused or injured a staff member either verbally or physically.**
- **Mutual agreement**
- **Or any event that is under violation, unethical or subject to closure of client relationship to secure the reputation of ADME and to comply with regulatory laws.**
- **Knowingly, client cheque gets dishonored or he/she issues stop payment instruction to his/her bank or cash transaction rejection request receive due to change in the currency at which cause a benefit to the client and loss ADME.**

ADME encounter with any situation mention above will consider exiting relationship with customers and also committed to report the incidents to regulatory organization. Additionally, input the names in Internal Blacklist master to assure the Client Exit process.

SOCIETIES AND CHARITY ORGANIZATIONS

ADME will not conduct foreign money transfers on behalf of any charity organization unless supported by an original certificate signed by H.E. the Minister of Social Affairs, permitting the concerned charity to collect donations and execute foreign transfers.

"ADME will not deal with any shell bank or shell company".

FINANCIAL INSTITUTIONS

The operation manager must, after undertaking EDD, obtain approval from the Chief Compliance Officer, the Manager in Charge "General Manager" and a member of the Owner for establishing a business relationship with any legal financial institution based in the United Arab Emirates While conducting EDD for exchange houses located inside UAE, ADME will follow the similar procedure which have establish for legal entities on-boarding, addition to this, the staff must collect following documents prior to get an approval from the Chief Compliance Officer, the Manager In Charge and Owner.

- **Central Bank of the UAE license**
- **AML Questionnaire**
- **CDD Questionnaire**
- **UBO's Information**
- **Senior Management and Ownership Structure**
- **Compliance Officer Details**
- **AED bank account details**
- **AML Policy and KYC Procedure (if applicable)**
- **Financial institution on-boarding booklet**
- **On Site Visit Report**

Sanctions Screening ADME

ADME adheres to Sanction laws and programs of various nations and intergovernmental bodies. Our program laws and regulations include and follow several obligations and expectations such as those managed by the and Central bank of the UAE, United Nations local regulatory US Treasury Department's Office of Foreign Assets Control (OFAC) and EU Sanctions.

ADME follows the instructions provided in the 'search notices' immediately in case the name of a party to a transaction is an exact match to a name or names in such notices issued by the Central Bank.

Following procedures must be strictly adhered to:

- **Maintain logs/records related to the clearing of potential sanction matches and keep them available in the system for five (5) years.**
- **Screen transactions against watch/sanctions lists such as Central Bank of UAE, United Nations, European Union, UK's HM Treasury and US's OFAC.**
- **Conduct Sanctions Compliance training program for all our employees.**
- **Not deal with any person/entity which may result in violation of any sanctions regulations.**
- **Introduce written processes and procedures for the escalation and clearing of potential sanction matches.**
- **Regular and automatic update of the UN sanction lists within the Point of Sale or computer systems without any manual intervention.**
- **Immediate update of changes pertaining to addition and deletion of names in the UN Sanctions list or CBUAE as when such changes are announced should also maintain appropriate logs into the system to confirm such updates.**
- **In case the name of a customer is an exact match (i.e., a true match) to a name or names in the UN Sanction lists or 'search and freeze notices' issued by the Central Bank, ADME must immediately freeze the funds of such customer, must inform the FIU along with the details of the customer and the amount of funds for further instructions. ADME must not unfreeze such amounts without obtaining a confirmation from the FIU.**
- **If the name of a party to a transaction is an exact match to a name or names in 'search notices' issued by the Central bank, ADME must immediately follow the instruction provided in such CB notices.**
- **Apply sanction screening against the customer's name in case of foreign currency exchange transactions.**
- **Apply sanction screening in case of money transfer transactions, where the Remitter's name and Beneficiary's name as well as the name of beneficiary bank should be screened against the sanction lists.**
- **In case of transactions conducted by a legal entity, the name of the authorized person who carried out the transaction (i.e., representative) must be screened against sanctions lists in addition to the name of the entity and its Beneficial Owner.**
- **ADME must strictly comply with the sanction screening requirements in case of third-party transactions.**

ACURIS Risk Intelligence

At ADME, the core operating system is synchronized with the up-to-date SDN Lists in order to automatically match customers' details with blacklisted entities. Our Core Operation System and Transaction Monitoring is integrated with Acuris Risk Intelligence Data records for Blacklist and Sanction Screening which are updated daily from their respective sources and server links.

Specifically, ADME is committed:

- **To require from commercial customers a separate Declaration Form confirming that their transactions have no direct or indirect relations with sanctioned countries and they do not act on behalf of any third party in facilitating remittances/payments**
- **To prohibit any transactions to and from sanctioned countries**
- **To report breaches of sanctions to the relevant regulatory authority**

Prohibition transactions

Prohibiting business activity, including prohibitions on commencing or continuing customer relationships or providing products or services or facilitating transactions that ADME believes may violate applicable sanctions laws or ADME. This includes individuals or entities named on a sanctions list or activity, directly or indirectly, involving countries or territories subject to comprehensive sanctions. These countries and territories include:

- Iran
- North Korea
- Myanmar
- Crimea

Customer Screening

- To comply with the anti-money laundering laws and regulations as well as the Central Bank directives, ADME is obliged to perform screening of all customers and block any transactions carried out by entities who have been identified on the sanctions lists (list includes, but shall not be restricted to UN, OFAC, CBUAE list and PEP list Furthermore, any suspicious transaction or a customer who is matched 100 % against a blacklisted entity has to be reported to the FIU via GO AML System.
- ADME core operating system has been integrated with Acuris Risk Intelligence and internal watch list and it is also linked with the following databases:

Screening Procedure "Customer Onboarding"

- The screening procedures are mandatory prior completion of corporate or individual customer onboarding
- Customer details are automatically checked against Acuris Risk Intelligence database and internal watch list once they are entered to the system
- The registration process may not be completed if a customer is identified as a potential match against any black list
- In case of any doubts or a potential match, the registration has to be put on hold until the customer is cleared of any suspicion
- The CO/ACO is responsible for the verification of screening alerts
- Customer screening is performed based on the name, date of birth, nationality and ID number of the customer
- If the validation indicates that the customer has no relation with the listed entity, the Compliance Officer / Alternate Compliance officer (in absence of CO) authorizes the customer registration in order to complete the onboarding process.
- If the validation of the customer details with those of the listed entity is not possible, the Compliance Officer/ACO requests more information from the branch. Having received additional clarification, the Compliance Officer/ACO validates the customer details and either authorizes or denies the customer registration
- The investigation procedures should be recorded as documentary evidence.

Foreign PEP (FPEP) and Head of International Organization (HIO) Checks

FPEP screening is the screening of customer names and associated details against FPEP information at certain points during the customer relationship. While some relevant, competent authorities do publish PEP lists, this is the exception rather than the norm as PEP lists are usually compiled internally or sourced from vendors/list providers. FPEP screening should occur in accordance with an FI's risk appetite applying an RBA and take place at least:

- As part of the on-boarding process
- At periodic customer review

- When there is a trigger event which warrants a customer due diligence review

As a minimum, PEP screening should be undertaken on those parties who are subject to identification requirements to meet KYC and CDD standards. This could include, but is not limited to: account holders, beneficial owners (including settlors, named and vested beneficiaries) and individuals with control over the account.

Screening Procedure: Transactions

- Each transaction conducted by corporate or individual customers is a subject of automatic verification against blacklists database.
- The screening process is broader than during the onboarding as it includes not only the customer details such as the name, date of birth, nationality and ID number but also the counterparty details.
- Sender/receiver details are automatically checked against Acuris Risk Intelligence database.
- The transaction process may not be completed if either a sender or receiver is identified as a potential match against any blacklist
- In case of any doubts or a potential match, the transaction has to be put on hold until both transaction parties are cleared of any suspicion
- The Compliance Department is responsible for the verification of screening alerts.
- If the validation indicates that the sender/receiver has no relation with the listed entity, the Compliance Team authorizes the transaction in order to complete the payment process.
- If the validation of the sender/receiver details with those of the listed entity is not possible, the Compliance Department requests more information from the branch. Having received additional clarification, the Compliance Officer validates the details and either authorizes or rejects the transaction.
- The investigation procedures should be recorded and maintained as documentary evidence.
- Any unusual or suspicious transactions as well as blacklisted entities have to be reported to the UAE Central Bank –Financial Intelligence Unit (FIU) by submitting a Suspicious Transaction Report (STR).
- All suspicious transactions must be placed on hold until any investigations are concluded
- All the information relating to the suspicious case has to remain confidential.
- Al Dhahery Money Exchange maintains its internal watch list that includes high risk and suspicious customers with whom the relationship is paused and transactions may not be processed.
- Remitter and Beneficiary bank got through sanction screening system.

Employee Screening (KYE- Know Your Employee)

Employees are the most important assets in the company. In order to ensure that these assets are also our most powerful defense against money laundering we should recruit employees with high level of integrity and ethics.

ADME takes below listed measures before hiring the employee:

- All employees must be screen once in a year.
- Potential employees must be screen regularly.
- New employees screening must be done prior to on boarding.
- A background check to ensure that there are no criminal records shall be conducted.

Blacklist Management

ADME shall maintain a Blacklist at its institution.

Blacklist:
True match against Central Bank of UAE, OFAC, UN, and EU sanctions lists or freeze notices issued by a competent authority in the UAE and against an internal watch list, names will be added into Internal Blacklist. The list will be maintained by the compliance department and system-based log will be maintained for audit trail.

Identifying and Blocking (or Freezing) Assets

Compliance team shall investigate on the potential sanction screening matches and queries escalated through IEMS or notices from competent law enforcement bodies. ADME maintaining internal black list register against sanction list or freeze notices issued by regulatory authority in the UAE. ADME will not continue or start any relationship with these customers in future unless there is a unfreeze notice from competent authority. If there any existing true match found on searched customer in ADME system, customer will escalate for Client Exit process.

Risk Based Approach

ADME will apply a risk-based approach to identify, assess, monitor, manage and mitigate AML and CTF risk.

- **Where higher risk is identified, enhanced measures are required to manage and mitigate those risks.**
- **Domestic PEP's will consider as a customer referring to Cabinet Decision No. (10) of 2019 Concerning the implementing regulation of decree law no. (20) of 2018 on anti- money laundering and combating the financing of terrorism and illegal organization. Dealing with Domestic PEP's is subject to the Senior Management approval.**
- **More rigorous requirements on the information which must accompany wire transfers, including information on the both the beneficiary and originator.**
- **ADME shall monitor Corporate Entities profiles more closely irrespective of their profile, structure, size, formation. Customers engaged in the business of Dealing in precious metals, dealers in real estate, dealers in luxury goods, auction houses, private banking customers, offshore companies, nonresident account holders, lawyers, notaries, and other independent legal professionals and accountants, trust and company service providers are intolerable to do business.**
- **The Compliance Department at corporate office will conduct annual review on high-risk customers. They will review system generated reports and review customers' transactions history.**

High Risk Customers Segment at ADME includes but are not necessarily limited to:

- **Customers who are identified as Politically Exposed Persons ("PEPs") or linked to Politically Exposed Persons ("PEPs")**
- **Customers on which there is adverse media negative news**
- **Customers linked to landlocked countries**

- **Any unusual pattern of transaction where the amounts are not consistent with the nature of business**
- **Multiple numbers of beneficiaries.**
- **If the beneficiaries are from non-exporting countries.**
- **New Beneficiaries registered every month which is not consistent to the nature of the customers' business.**

- **Non Resident customer as per the NRA.**

Enterprise-wide Money Laundering / Terrorism Financing Risk Assessment

Effective AML/CFT and Sanctions Compliance systems and controls are required to guard the organization against the risks of money laundering ("ML"), tax evasion and terrorist financing ("TF"). Both financial institutions and non-financial institutions are faced with an increasingly regulated environment, heightened regulatory scrutiny and complexity of AML/CFT and sanctions requirements at local and international levels. An Institutional ML/TF Risk Assessment also known as Enterprise-Wide ML/TF Risk Assessment (EWRA) forms the basis for applying an RBA to AML/CFT compliance programmed.

ADME Enterprise-Wide ML/TF Risk Assessment allows to demonstrate how, and to what extent they are vulnerable to ML/TF risks, how they currently mitigate these risks, therefore allowing them to adopt appropriate measures to manage any residual risks according to the organization's risk appetite. The objectives of EWRA as follows

To assess the Inherent Risk

Must consider all relevant inherent risk factors at the customer/entity, products/services, transactions, channels, and geographical level. The assessment must be performed in a holistic manner.

To assess the Mitigating Controls

Enables financial institutions to understand how and to what extent, they are vulnerable to ML/TF -> measuring the exposure to ML/TF through an assessment of the mitigating controls. These are assed across various control categories, e.g., corporate governance, KYC/CDD/EDD, STR reporting, training and record keeping.

To assessment the Residual Risk

The Residual Risk is obtained by taking into account the inherent risk and the overall controls rating.
More recently, crimes such as insider dealing and market manipulation have become predicate offences to money laundering and, as such, could be considered in the context of a ML risk assessment. For the time being, however, these are generally considered separately from a ML risk assessment although the methodology used to assess the risks presented is similar.

ADME Risk Assessment

Ownership

ADME overall risk assessment (EWRA) exercise is carried out under the responsibility of the CCO that ensures related procedures and processes are formalized and executed in a manner that reflects the results of this permanent exercise. The ADME identifies and classifies the ML/TF risks.

Risk Identification:

EWRA Areas Well-thought-out for ADME

- **Individuals bringing currencies frequently from cross border**
- **Risky currencies which are mostly target of Money launderers**
- **Tourist customers from high-risk jurisdictions**
- **Counterparty exchange house internal compliance controls**
- **UBO's as corporate clients which are not very much transparent**
- **Distortion in currency markets specially for most demanding currencies like USD etc.**
- **Rapid Staff turnover specially in compliance**
- **Less improvement in Remittance business**
- **Regulatory risk reporting category alarming as "Medium High Risk"**
- **Overall business covering High Risk customers**
- **Risk arising through gold market customers**
- **Free zone corporate customers with opaque ownership and complex structure.**

GAP Analysis: ADME will conduct frequent gap analysis to understand the complexity of its business by applying equation: Inherent Risk- Control effectiveness= Residual Risk

Risk Appetite: ADME will understand its risk appetite by the complicity and size of business. ADME is not allowed to keep its risk appetite high and increased residual risk.

Adjustment Phase: ADME will keep reviewing the applied controls effectiveness and will apply additional controls whenever it will be required.

RBA Application

ADME applied RBA characteristics of their customers, the products, services or operations they offer, the countries or geographical areas concerned, as well as the distribution channel.

High Risk = EDD

Medium Risk = Additional EDD

Low Risk = Standard Due diligence

Risk Methodology

Risk Management Methodology

Risk Assessment is method used in our Exchange to identify possible risks or vulnerabilities of its customers to an organization. Risk rating or customer profiling is an ongoing process that begins when onboarding a customer.

During the transaction, the profile undergoes further reviews and analysis of the results for the transactional risk assessment. In Al Dhahery Money Exchange, we identify, assess and understand the risks associated with money laundering. We have also implemented the methodology of risk assessment according to size, nature, and complexity of the business to assess the risk.

Types of Risk

The risks of money laundering can be measured by different categories, which can be altered by risk variables.

Following are the risk criteria used in Enterprise-Wide Risk and Risk Based Approached Model. The risk assessment should cover all relevant factors including:

- **Customer risk**
- **Products and services risk**
- **Delivery channel risk**
- **New technologies risk**
- **Jurisdiction or geographic risk**

- **Counterparty risk**
- **Other areas of risk**

Customer Risk

Factors that may determine that a customer poses a higher risk include the list below, which is not exhaustive and may also consider other factors:

- **Difficult to identify true owners of the company;**
- **Senior Management positions occupied by individuals or their close relatives who are politically exposed or part of government corporations;**
- **Identified to be involved in support of terrorist activities;**
- **NGO's or 'Non – profit' organizations;**
- **Dealing in high-risk items;**
- **Customer process unusual transaction without proper explanation.**

Services / Product Risk

Service/Product risks are risks associated with products or services offered by the organization. ADME must assess and document the risks of money laundering, terrorism financing and other illicit activities posed by the types of products it offers. Some of the examples are below, which is not exhaustive and may also consider other factors:

- **Cross border services providing extra anonymity, including Correspondent or international private banking Banknotes or precious metal trading;**
- **Customer deals in general trading or occupying general trading license.**

Delivery Channel Risk or Interface Risk

A delivery channel is a medium that can be used to obtain a product or service, or through which transactions can be conducted. Delivery channels should be considered as part of the risk of the transactions, given the potential impact of new developments and technologies. Delivery channels that allow for non-face-to-face transactions pose a higher inherent risk. Non face to face transaction poses higher risk service because it can allow unidentified parties to conduct transactions.

New technologies risk

ADME FLA must identify, assess, understand, and mitigate the ML/FT risk to which they may be exposed by new technologies, including new delivery mechanisms such as mobile and online remittance.

Jurisdiction / Geographical Risk

Factors that may indicate that a country poses a higher risk include the list below, which is not exhaustive and may also consider other factors:

- **Sanction Countries;**
- **Countries identified to be involved in supporting of terrorist activities;**
- **Countries identified by FATF or identified from other trusted sources having an inappropriate money laundering laws and regulations controls;**

- Countries identified with weak governing laws and regulations to combat terrorist financing;
- Countries identified by credible sources as having significant levels of corruption or being a non-transparent tax environment.
- Countries at High Risk are considered as high risk and are required additional examinations like sanction check, google search to explore adverse media. In case, if required, we conduct cross verification of given documents if the transaction owner/beneficiary of those countries.

Counterparty Risk

Counterparty Risk is the likelihood or probability that one of those involved in a transaction might default on its contractual obligation. One of the main risks associated with correspondent banking is the fact that the correspondent often has no direct relationships with the underlying parties to a transaction and is therefore not in a position to verify their identities or conduct the necessary due diligence.

Other areas of risk.

ADME shall document risk assessment methodology, process and findings. Determine the level of, acceptable level of risk and mitigation measures to be applied to minimize the impact of risks. Other areas of illicit finance risk, including sanctions and proliferation financing.

Risk Scoring Methodology and Procedures

The risk of the customer and transaction shall be calculated based on the below parameters and its scoring. Each transaction and customer profile shall be assessed on transaction frequency (parameter set for no. of transactions), Transaction Amount Risk Score (slabs of amounts), Transaction Type, Remitter Type Risk Score, Country Risk Score, Service Type / Counterparty Risk and Delivery Channel Risk.

Onboarding and Transactional Risk Scoring Methodology

Individuals and corporates will be given a risk score based on the following:

1. **Onboarding Risk**
2. **Transaction Risk**
3. **Profile Risk**

Individual and Corporate weightage is assigned to each factor as mentioned below:

Risk Type	Weightage
Onboarding	35
Transaction	30
Profile	35
Total	100

INDIVIDUAL ACCOUNTS

Onboarding Risk – Individuals

Weightage for onboarding is 35

Onboarding Risk for Individuals are based on the following parameters:

1. **Country of Birth/ Place of Birth (Refer to annexure 1.1)**
2. **Nationality Refer to annexure 1.1)**
3. **Nature of Business (Refer to annexure 1.3)**
4. **Occupation (Refer to annexure 1.2)**
5. **PEP Status: Y=10 N=1**
6. **Resident Status: Non-Resident=10 Resident=1**

Weightage can be assigned to each factor or parameter. At Al Dhahery Money Exchange, we have given below weightage for each parameter:

Sl#	Parameters	Rating	Weightage
1	Nationality	Ref. Nationality	15
2	Country of Birth	Ref. Country	15
3	Occupation	Ref. Occupation	10
4	Nature of Business	Ref. Business	10
5	Resident Status	Non Resident=10 Resident=1	15
6	PEP/Adverse Media	Y=10 N=1	25
7	Blacklist	Blacklist	10
	Total Weightage		100

Sl#	Parameters	Rating	Weightage
1	Company Type	Ref. Company Types	10
2	Mainland/Freezone	Mainland Then 1.00; Freezone Then 10.00	8
3	Number of Years in Business	<=1 Then 10.00; <=2 Then 5.00; >=3 Then 1.00	8
4	Nature of Business	Ref. Business Types	8
5	Nature of Business Sub type	Ref. Business Types	8
6	KYC Document Docket	Ref. KYC Document Docket	9
7	Owner/Partner's Nationality	Ref. Country List	9
8	Representative's Nationality	Ref. Country List	8
9	Tenure of relationship	<=1 Then 10.00; <=5 Then 5.00; >5 Then 1.00	8
10	Country of Registration	Ref. Country List	8
11	Screening Docket	Ref. Company Screening	8
12	Blacklist	Blacklist	8
	Total Weightage		100

Sample of the computation for Onboarding Risk is shown below:

Sl No	Type	Weightage	Score	Value	Rate
1	Blacklist	10	7.00	70.00	MEDIUM HIGH
2	Country Of Birth	15	10.00	150.00	HIGH
3	Nationality	15	10.00	150.00	HIGH
4	Nature of Buisines	10	10.00	100.00	HIGH
5	Occupation	10	5.00	50.00	MEDIUM
6	PEP/Adverse Media	25	1.00	25.00	LOW
7	Resident	15	10.00	150.00	HIGH
		100	53.00	695.00	

Onboarding Risk Score 695.00 / 100 = 6.950000 Tran. Onboarding Risk Score (6.95 * 35) / 100 = 2.4325

$$\text{Onboarding Risk (OR)} = \frac{(\text{Total Value}/\text{ Total Weightage})^* (\text{ Weightage of Onboarding Risk})}{100}$$

**Weightage of Onboarding Risk= 35

Transaction Wise Risk for Individuals

Weightage for Transaction is 30

Transaction Risk for Individuals is based on following factors:

1. **Amount Risk (Refer to annexure 1.5)**
2. **Beneficiary Nationality (Refer to annexure 1.1)**
3. **Delivery Channel (Refer to annexure 1.8)**
4. **Destination Country (Refer to Annexure 1.1)**
5. **Face to Face: Yes=1, No=10**
6. **Frequency Risk (Refer to Annexure 1.6)**
7. **Payment Mode: Cash=10, non-Cash= 5**
8. **Product Risk (Refer to Annexure 1.4)**
9. **Service Type Risk (Refer to Annexure 1.7)**

Weightage can be assigned to each factor and depending on customers mode of operation, for example, assigning a weightage of zero to a factor, would mean that the factor is not considered in the risk score. In Al Dhahery Money Exchange, we have given below weightage for each parameter.

Parameters	Weightage
1. Amount Risk	20
2. Beneficiary Nationality	10
3. Delivery Channel	9
4. Destination Country	10
5. Face to Face	9
6. Frequency Risk	15
7. Payment Mode	9
8. Product Risk	9
9. Service Type Risk	9
TOTAL	100

Sample of the computation for Transaction-Wise Risk is shown below:

Transaction WISE RISK

Sl No	Type	Weightage	Score	Value	Rate
1	Amount Risk	20	3.00	60.00	LOW
2	Face to Face	9	1.00	9.00	LOW
3	Frequency Risk	15	5.00	75.00	MEDIUM
4	Payment Mode	9	10.00	90.00	HIGH
5	Product Risk	9	8.00	72.00	HIGH
		62	27.00	306.00	

Transaction Risk Score 306.00 / 62 = 4.935484 Tran. Transaction Risk Score (4.935484 * 30) / 100 = 1.4806452

$$\text{Transaction Wise Risk (TR)} = \frac{(\text{Total Value} / \text{Total Weightage}) * (\text{Weightage of Transaction Wise Risk})}{100}$$

**Weightage of Transaction Wise Risk= 30

Profile Risk for Individuals

Weightage for Profile is 35

Profile Risk for Individuals is based on below factors/parameters:

Sl No.	Parameters	Rule	Rating	Weightage	Description
1	New Beneficiary	>=3 in Month	10	8	If new beneficiary in a month greater than or equal 3 then score will 10 otherwise it will be zero
2	High risk currencies	75000	10	8	If the High-risk currency greater than 75000 then score will be 10 otherwise be zero
3	Availing another product	>1	10	8	if more than one product then the score will be 10 else it will be zero
4	Sending to high-risk country frequency	>=3 Month	10	10	If the high-risk country frequency greater than or equal 3 then score will be 10 otherwise it will be zero
5	New Customer carrying out large transaction	once in a quarter	10	10	If the Transaction Amount is greater than previous large amount in the quarter then score will be 10 otherwise it will be zero
6	Number of cancelled transactions	>=3	10	8	If the No. of cancelled transaction greater than or equal to 3 then the score will be 10 otherwise it will be zero
7	Customer sending to many beneficiaries	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
8	Customer receiving from high-risk country	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
9	Customer sending to multiple countries – outward	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
10	Customer receiving from multiple countries – inward	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
11	Exchange of currency	No of currencies	3<: 5, 3-4: 8, >4: 10	8	If the No. of currencies below 3 then score will be 5, No. of currencies between 3 to 4 then score will be 8, And No. of currencies above 4 then score will be 10
12	Customer Volume	Average monthly value of FC/Remittance	3000<: 5, 3000-99,999.99: 8, >100,000: 10	8	If the Average Amount below 3000 then score will be 5, Average Amount between 3000 to 10000 then score will be 8, And No. of transaction above 10000 then score will be 10
Total Weightage				100	

For Profile Risk, if parameters are not hit, they will not be shown in the calculation page. As per Cinque, this is the practice for all the exchange houses they're servicing. So, for example as seen below, only two (2) parameters are hit out of 12 actual parameters, so the calculation page will show two (2) parameters only.

Sample of the computation for Profile Risk is shown below:

PROFILE RISK

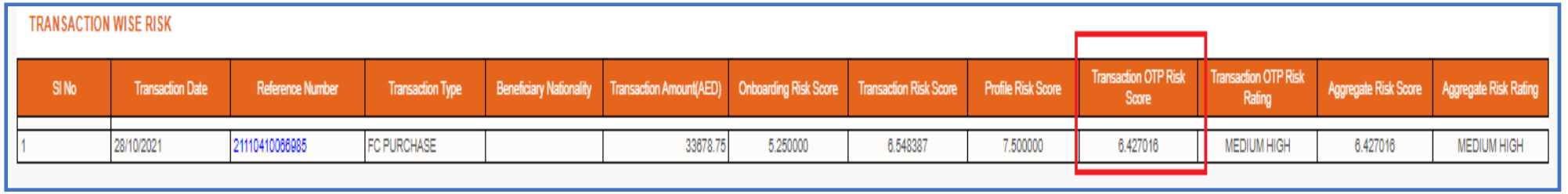
Sl No	Type	Weightage	Score	Value	Rate
1	Exchange of currency	8	5.00	40.00	MEDIUM
2	Customer Volume	8	5.00	40.00	MEDIUM
		16	10.00	80.00	

Profile Risk Score 80.00 / 16 = 5.000000 Tran. Profile Risk Score (5.00 * 35) / 100 = 1.75

$$\text{Profile Risk (PR)} = \frac{(\text{Total Value}/\text{ Total Weightage})^* (\text{ Weightage of Profile Risk})}{100}$$

**Weightage of Profile Risk= 35

Overall Customer OTP Risk Score = OR+TR+PR



TRANSACTION WISE RISK

Sl No	Transaction Date	Reference Number	Transaction Type	Beneficiary Nationality	Transaction Amount(AED)	Onboarding Risk Score	Transaction Risk Score	Profile Risk Score	Transaction OTP Risk Score	Transaction OTP Risk Rating	Aggregate Risk Score	Aggregate Risk Rating
1	28/10/2021	21110410066985	FC PURCHASE		33678.75	5.250000	6.548387	7.500000	6.427016	MEDIUM HIGH	6.427016	MEDIUM HIGH

Aggregate Risk Score:

The current Aggregate Risk Score is the average score of all aggregate risk score for each transaction.

SCORING LEGEND

Risk Rating	Risk Range		Risk Rating	Risk Range
Low Risk	**0.00 To 3.00**		Medium High Risk	**5.01 To 7.00**
Medium Risk	**3.01 To 5.00**		High Risk	**7.01 To 10.00**

Customer Risk is Overridden

** Non Resident customer as High Risk*

CUSTOMER PROFILE

Member Type	REGISTERED MEMBER	Customer Code	29393
Salutation	Mr.	Opened Date	13/06/2022
Full Name	ELSAID ABDELHAMID MOHAMED REZK		
Customer Type	INDIVIDUAL	Date of Birth	22/03/1963
Gender	MALE	Birth Place	DAKAHLIYA
Mobile Number	201007530330	Phone Number	
Designation	Business Owner	Company	ASTRA OFFICE FOR IMPORT AND EXPORT
Address 1	SUN AND SANDS HOTEL RM 164	Address 2	BANIYAS DEIRA DUBAI
State	DUBAI	Country	AE
Country of Birth	EGYPT	Created By	1024
Created On	6/13/2022 10:01:31 AM		

10.00 / 10.00

Current Aggregate Risk

HIGH

10.00 / 10.00

On boarding Risk

HIGH

CUSTOMER ONBOARDING RISK SCORING

Factor		Risk Score	Risk Rate
Nationality	EGYPT	5.00	MEDIUM
Country of Birth	EGYPT	5.00	MEDIUM
Occupation	BUSINESSMAN	10.00	HIGH
Nature of Business	Import and export	10.00	HIGH
Resident Status	NON-RESIDENT	10.00	HIGH
PEP Status	No	1.00	LOW
Blacklist	0.00	3.00	LOW
		Onboarding Risk Score	10.00 / 10.00

Note: **For an individual irrespective of the score as per the legend, there is an overriding rule in the system, if resident status is "Nonresident" which is marked as "HIGH" or the nationality is marked "HIGH" as per NRA guidelines, CURRENT AGGREGATE RISK and ONBOARDING RISK will be automatically "HIGH". Sample Below:**

SCORING LEGEND

Risk Rating	Risk Range		Risk Rating	Risk Range
Low Risk	**0.00 To 3.00**		**Medium High Risk**	**5.01 To 7.00**
Medium Risk	**3.01 To 5.00**		**High Risk**	**7.01 To 10.00**

Customer Risk is Overridden

** High Risk Nationality*
** Company type is in 0*
** Nature Of Business is in HIGH*

CUSTOMER PROFILE

Member Type	REGISTERED MEMBER	**Customer Code**	69988
		Opened Date	17/06/2023
Full Name	ZAM ZAM JEWELLERY LLC		
Customer Type	CORPORATE	**Date of Est.**	30/10/2005
Mobile Number	042724007	**Phone Number**	
Address 1	SHOP NO 6 AL BUTAIN AUH BUILDING	**Address 2**	
State	DEIRA	**Country**	AE
Country of Inc.	UNITED ARAB EMIRATES	**Created By**	1055
Created On	6/17/2023 9:40:14 AM		

10.00 / 10.00

Current Aggregate Risk
HIGH

10.00 / 10.00

On boarding Risk
HIGH

CUSTOMER ONBOARDING RISK SCORING

Factor		Risk Score	Risk Rate
Company Type	Limited liability company	10.00	HIGH
Mainland / Free Zone Company	NO	1.00	LOW
No of Years in Business	>=3	1.00	LOW
Nature of Business	Jewelry items trading	10.00	HIGH
Business Sub Type	Small Medium Enterprise (SME)	8.00	HIGH
KYC Dockets		0.00	LOW
Owner Nationality		5.00	MEDIUM
Representative Nationality		5.00	MEDIUM
Tenure of Relationship	1	10.00	HIGH
Country of Registration	United Arab Emirates	10.00	HIGH
Screening Dockets		0.00	LOW
Blacklist	0.00	3.00	LOW
		Onboarding Risk Score	10.00 / 10.00

We have categorized our risk into four categories: Low, Medium, Medium High & High Risk. After the customer is onboarded and the transaction is executed, the current aggregate risk score of the customer may change as per the parameters set in the system consolidating onboarding Risk score, Transactional risk score & profile risk score.

Score Legend for Individual is illustrated below:

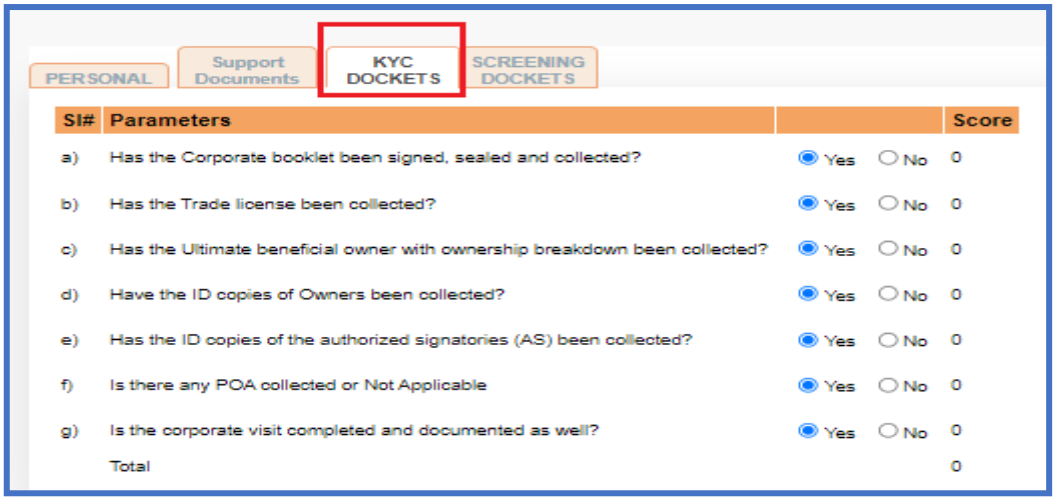
CORPORATE ACCOUNTS

Onboarding Risk – Corporates

Weightage for onboarding is 35

Onboarding Risk is based on following factors/parameters:

1. **Company Type (Refer to Annexure 1.9)**
2. **Mainland/ Free zone - 1 Free zone = 10**
3. **Number of years in business: ≤1=10, ≤2=5, ≥3=1**
4. **Nature of Business (Business Sector) (Refer to Annexure 1.10)**
5. **Nature of Business Sub type (Refer to Annexure 1.11)**
6. **KYC Document Docket- "By Default-Yes" but if any of the parameter is hit, it should be ticked manually.**



7. **Owner/ Partner's Nationality (Refer to Annexure 1.1)**
8. **Representative's Nationality (Refer to Annexure 1.1)**
9. **Tenure of relationship: <=1, score is 10; <=5, score is 5; >5, score is 1**
10. **Country of company registration (if applicable) (Refer to Annexure 1.1)**
11. **Screening Dockets – "By Default- No" for Parameters A-K & M-P and "By Default- Yes" for parameter L. But if any parameter is hit, it should be ticked otherwise manually.**

PERSONAL | Support Documents | KYC DOCKETS | SCREENING DOCKETS

Sl#	Parameters		Score
a)	Is there a PEP or associates of PEPs in the corporate's Owners, Board of Directors or Sr. Management?	○ Yes ◉ No	0
b)	Is there negative (Adverse Media/Fraud) news on the Owners, Board of Directors or Sr. Management or company?	○ Yes ◉ No	0
c)	Does the Company name or Subsidiary/Affiliate entities feature in any sanctions list?	○ Yes ◉ No	0
d)	Are there any sanctions against the Owners, Board of directors, or Sr. Management of the company?	○ Yes ◉ No	0
e)	Is there a sanction in force on the Country of Nationality of Owners/ Partners/Board of Directors/Sr. Managements'?	○ Yes ◉ No	0
f)	Is the company owned by entities located in sanction/FATF restricted areas?	○ Yes ◉ No	0
g)	Does the entity have any presence like branches/subsidiaries/representative offices in sanction/FATF restricted areas?	○ Yes ◉ No	0
h)	Does the corporate have relationship with any other high-risk Entity?	○ Yes ◉ No	0
i)	Were any suspicious activities noticed and reported on representative/BOD/Sr. Management of the corporate transacting as individuals, etc.?	○ Yes ◉ No	0
j)	Were there any red flags on Corporate's behavior while interacting or providing necessary documents?	○ Yes ◉ No	0
k)	Are there any unusual actives (Over/Under invoicing, Over/Under Shipment, Over/Under Pricing, Multiple Invoicing and False Invoicing)?	○ Yes ◉ No	0
l)	Has the Bank statements or Annual Report Collected from Client?	◉ Yes ○ No	0
m)	Does the Corporate intend to deal with sanction Countries?	○ Yes ◉ No	0
n)	Does the Corporate intend to deal with any FATF listed High Risk Countries?	○ Yes ◉ No	0
o)	Corporate intend to deal with the country listed as per Basel Index Rating?	○ Yes ◉ No	0
p)	Jurisdiction of parent company (if applicable)	○ Yes ◉ No	0
	Total		0

Weightage can be assigned to each factor or parameter. At Al Dhahery Money Exchange, we have given below weightage for each parameter:

Sl#	Parameters	Rating	Weightage
1	Company Type	Ref. Company Types	10
2	Mainland/Freezone	Mainland Then 1.00; Freezone Then 10.00	8
3	Number of Years in Business	<=1 Then 10.00; <=2 Then 5.00; >=3 Then 1.00	8
4	Nature of Business	Ref. Business Types	8
5	Nature of Business Sub type	Ref. Business Types	8
6	KYC Document Docket	Ref. KYC Document Docket	9
7	Owner/Partner's Nationality	Ref. Country List	9
8	Representative's Nationality	Ref. Country List	8
9	Tenure of relationship	<=1 Then 10.00; <=5 Then 5.00; >5 Then 1.00	8
10	Country of Registration	Ref. Country List	8
11	Screening Docket	Ref. Company Screening	8
12	Blacklist	Blacklist	8
	Total Weightage		100

Sample of the computation for Onboarding Risk is shown below:

Factor		Risk Score	Risk Rate
Company Type	Limited liability company	10.00	HIGH
Mainland / Free Zone Company	NO	1.00	LOW
No of Years in Business	>=3	1.00	LOW
Nature of Business	Jewelry items trading	10.00	HIGH
Business Sub Type	Small Medium Enterprise (SME)	8.00	HIGH
KYC Dockets		0.00	LOW
Owner Nationality		5.00	MEDIUM
Representative Nationality		5.00	MEDIUM
Tenure of Relationship	1	10.00	HIGH
Country of Registration	United Arab Emirates	10.00	HIGH
Screening Dockets		0.00	LOW
Blacklist	0.00	3.00	LOW
		Onboarding Risk Score	10.00 / 10.00

$$\text{Onboarding Risk (OR)} = \frac{(\text{Total Value}/\text{ Total Weightage})^* (\text{ Weightage of Onboarding Risk})}{100}$$

**Weightage of Onboarding Risk= 35

We have categorized also for our corporate accounts, the risks into four categories: Low, Medium, Medium High & High Risk. After the customer is onboarded and the transaction is executed, the current aggregate risk score of the customer may change as per the parameters set in the system consolidating onboarding Risk score, Transactional risk score & profile risk score.

Note: Whenever the company type selected is between the rating 9-10 (HIGH RISK TYPE) then the aggregate & Onboarding customer risk category will be automatically "HIGH", irrespective of the score as per the legend and this is in accordance with the guidelines of NRA. This is an overriding rule in the system and sample is shown below:

Transaction Risk for Corporate

Weightage for Transaction is 30

Transaction Risk for corporate is based on following factors:

1. **Amount Risk (Refer to Annexure 1.12)**
2. **Beneficiary Nationality (Refer to Annexure 1.1)**
3. **Delivery Channel (Refer to Annexure 1.8)**
4. **Destination Country (Refer to Annexure 1.1)**
5. **Frequency Risk (Refer to Annexure 1.13)**
6. **Payment Mode: Cash=5, Cheque=10**
7. **Product Risk (Refer to Annexure 1.4)**
8. **Sender Nationality (Refer to Annexure 1.1)**
9. **Service Type Risk (Refer to Annexure 1.7)**

Weightage can be assigned to each factor and depending on customers mode of operation, for example, assigning a weightage of zero to a factor, would mean that the factor is not considered in the risk score. In Al Dhahery Money Exchange, we have given below weightage for each parameter.

Parameters	Weightage

1. Amount Risk	**20**
2. Beneficiary Nationality	**10**
3. Delivery Channel	**9**
4. Destination Country	**10**
5. Frequency Risk	**15**
6. Payment Mode	**9**
7. Product Risk	**9**
8. Sender Nationality	**9**
9. Service Type Risk	**9**
TOTAL	**100**

Sample of the computation for Transaction-Wise Risk is shown below:

Sl No	Transaction Date	Reference Number	Transaction Type	Transaction Amount(AED)	Onboarding Risk Score	Transaction Risk Score	Profile Risk Score	Transaction OTP Risk Score	Transaction OTP Risk Rating	Aggregate Risk Score	Aggregate Risk Rating
1	15/11/2023	23110410057332	FC PURCHASE	19713.50	5.290000	7.629033	8.461537	7.101748	HIGH	7.220423	HIGH
2	13/11/2023	23110410056854	FC PURCHASE	18186.75	5.290000	7.629033	7.500000	6.765210	MEDIUM HIGH	7.223630	HIGH
3	08/11/2023	23110410056036	FC PURCHASE	4833.00	5.290000	7.629033	6.500000	6.415210	MEDIUM HIGH	7.236364	HIGH

$$\text{Transaction Wise Risk (TR)} = \frac{(\text{Total Value}/\text{ Total Weightage})^* (\text{ Weightage of Transaction Wise Risk})}{100}$$

**Weightage of Transaction Wise Risk= 30

Profile Risk for Corporate

Weightage for Profile Risk is 35

Profile Risk for corporate is based on below factors:

Sr No.	Parameters	Rule	Rating	Weightage	Description
1	New Beneficiary	>=3 in Month	10	8	If new beneficiary in a month greater than or equal 3 then score will 10 otherwise it will be zero
2	High risk currencies	75000	10	8	If the High-risk currency greater than 75000 then score will be 10 otherwise be zero
3	Availing another product	>1	10	8	if more than one product then the score will be 10 else it will be zero
4	Sending to high-risk country frequency	>=3 Month	10	10	If the high-risk country frequency greater than or equal 3 then score will be 10 otherwise it will be zero
5	New Customer carrying out large transaction	once in a quarter	10	10	If the Transaction Amount is greater than previous large amount in the quarter then score will be 10 otherwise it will be zero
6	Number of cancelled transactions	>=3	10	8	If the No. of cancelled transaction greater than or equal to 3 then the score will be 10 otherwise it will be zero
7	Customer sending to many beneficiaries	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10

8	Customer receiving from high-risk country	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
9	Customer sending to multiple countries – outward	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
10	Customer receiving from multiple countries – inward	Month	3<: 5, 3-4: 8, >4: 10	8	If the No. of transaction below 3 then score will be 5, No. of transaction between 3 to 4 then score will be 8, And No. of transaction above 4 then score will be 10
11	Exchange of currency	No of currencies	3<: 5, 3-4: 8, >4: 10	8	If the No. of currencies below 3 then score will be 5, No. of currencies between 3 to 4 then score will be 8, And No. of currencies above 4 then score will be 10
12	Customer Volume	Average monthly value of FC/Remittance	3000<: 5, 3000-99,999.99: 8, >100,000: 10	8	If the Average Amount below 3000 then score will be 5, Average Amount between 3000 to 10000 then score will be 8, And No. of transaction above 10000 then score will be 10
Total Weightage				100	

For Profile Risk, if parameters are not hit, they will not be shown in the calculation page. As per Cinque, this is the practice for all the exchange houses they're servicing. So, for example as seen below, only two (2) parameters are hit out of 12 actual parameters, so the calculation page will show two (2) parameters only.

Sample of the computation for Transaction-Wise Risk is shown below:

PROFILE RISK

Sl No	Type	Weightage	Score	Value	Rate
1	Exchange of currency	8	5.00	40.00	MEDIUM
2	Customer Volume	8	10.00	80.00	HIGH
		16	15.00	120.00	

Profile Risk Score 120.00 / 16 = 7.500000 Tran. Profile Risk Score (7.50 * 35) / 100 = 2.625

$$\text{Profile Risk (PR)} = \frac{\text{(Total Value/ Total Weightage)* (Weightage of Profile Risk)}}{100}$$

**Weightage of Profile Risk= 35

Overall Customer OTP Risk Score = OR+PR+TR

TRANSACTION WISE RISK

Sl No	Transaction Date	Reference Number	Transaction Type	Beneficiary Nationality	Transaction Amount(AED)	Onboarding Risk Score	Transaction Risk Score	Profile Risk Score	Transaction OTP Risk Score	Transaction OTP Risk Rating	Aggregate Risk Score	Aggregate Risk Rating
1	11/10/2021	21110420064123	FC SALES		1832250.00	5.050000	8.693547	7.500000	7.000564	MEDIUM HIGH	6.909965	HIGH

Aggregate Risk Score:

The current Aggregate Risk Score is the average score of all aggregate risk score for each transaction.

TRANSACTION WISE RISK

Sl No	Transaction Date	Reference Number	Transaction Type	Beneficiary Nationality	Transaction Amount(AED)	Onboarding Risk Score	Transaction Risk Score	Profile Risk Score	Transaction OTP Risk Score	Transaction OTP Risk Rating	Aggregate Risk Score	Aggregate Risk Rating
1	24/04/2023	23110410019321	FC PURCHASE		130818.75	5.950000	8.500000	7.500000	7.257500	HIGH	6.191095	HIGH
2	24/04/2023	23110410019275	FC PURCHASE		555997.75	5.950000	8.500000	8.461537	7.594038	HIGH	6.189341	HIGH
3	19/04/2023	23110410018901	FC PURCHASE		72268.00	5.950000	8.500000	7.500000	7.257500	HIGH	6.187027	HIGH
4	19/04/2023	23110410018899	FC PURCHASE		32709.75	5.950000	8.500000	7.500000	7.257500	HIGH	6.185261	HIGH
5	17/04/2023	23110410018608	FC PURCHASE		119432.00	5.950000	8.500000	7.500000	7.257500	HIGH	6.183489	HIGH
6	15/04/2023	23110410018380	FC PURCHASE		243791.00	5.950000	8.500000	7.500000	7.257500	HIGH	6.181710	HIGH
7	14/04/2023	23110410018280	FC PURCHASE		76872.25	5.950000	8.500000	7.500000	7.257500	HIGH	6.179926	HIGH
8	09/04/2023	23110410017489	FC PURCHASE		266998.75	5.950000	9.225807	7.500000	7.475242	HIGH	6.178136	HIGH
9	05/04/2023	23110410017020	FC PURCHASE		109344.25	5.950000	9.225807	7.500000	7.475242	HIGH	6.175978	HIGH
10	05/04/2023	23110410016971	FC PURCHASE		21458.75	5.950000	9.225807	7.500000	7.475242	HIGH	6.173813	HIGH
11	04/04/2023	23110410016837	FC PURCHASE		11699.00	5.950000	8.500000	7.500000	7.257500	HIGH	6.171640	HIGH
12	03/04/2023	23110410016626	FC PURCHASE		49402.75	5.950000	8.500000	7.500000	7.257500	HIGH	6.169824	HIGH
13	03/04/2023	23110410016625	FC PURCHASE		73854.25	5.950000	8.500000	7.500000	7.257500	HIGH	6.168002	HIGH
14	31/03/2023	23110410016296	FC PURCHASE		58591.75	5.950000	8.500000	7.500000	7.257500	HIGH	6.166174	HIGH
15	29/03/2023	23110410015966	FC PURCHASE		141615.75	5.950000	8.500000	7.500000	7.257500	HIGH	6.164340	HIGH
16	25/03/2023	23110410015348	FC PURCHASE		138874.75	5.950000	8.500000	7.500000	7.257500	HIGH	6.162500	HIGH
17	20/03/2023	23110410014519	FC PURCHASE		86563.25	5.950000	9.225807	7.500000	7.475242	HIGH	6.160653	HIGH
18	20/03/2023	23110410014449	FC PURCHASE		304609.00	5.950000	9.225807	8.461537	7.811780	HIGH	6.158433	HIGH
19	17/03/2023	23110410014089	FC PURCHASE		82282.50	5.950000	9.225807	8.461537	7.811780	HIGH	6.155635	HIGH
20	16/03/2023	23110410013782	FC PURCHASE		61803.25	5.950000	9.225807	7.500000	7.475242	HIGH	6.152828	HIGH
21	15/03/2023	23110410013620	FC PURCHASE		480871.00	5.950000	9.225807	8.461537	7.811780	HIGH	6.150583	HIGH
22	14/03/2023	23110410013462	FC PURCHASE		48002.75	5.950000	9.225807	7.500000	7.475242	HIGH	6.147758	HIGH
23	13/03/2023	23110410013218	FC PURCHASE		45112.75	5.950000	9.225807	7.500000	7.475242	HIGH	6.145496	HIGH
24	11/03/2023	23110410012881	FC PURCHASE		126451.00	5.950000	9.225807	7.500000	7.475242	HIGH	6.143227	HIGH
25	09/03/2023	23110410012516	FC PURCHASE		30016.00	5.950000	9.225807	7.500000	7.475242	HIGH	6.140950	HIGH
26	08/03/2023	23110410012378	FC PURCHASE		156501.25	5.950000	9.225807	7.500000	7.475242	HIGH	6.138665	HIGH
27	07/03/2023	23110410012121	FC PURCHASE		53992.00	5.950000	9.225807	7.500000	7.475242	HIGH	6.136373	HIGH

HOW TO HANDLE LOW, MEDIUM, MEDIUM-HIGH- & HIGH-RISK CUSTOMERS:

INDIVIDUAL CUSTOMERS:

KYC is being carried out to verify the identity of their clients in compliance with legal requirements and current laws and regulations. Know Your Customer is the due diligence that the Exchange House performs to identify their clients and ascertain relevant information pertinent to doing business with them. In Al Dhahery, we perform CID, CDD and EDD depending on the amount and type of transactions of the individual customers.

Basically, for all customers regardless of the risk ratings, cashiers need to collect valid physical ID, verify and upload in the system. So, KYC process must be applied. Once they put the name of the customer in the system, there will be an automatic sanction screening of the customer.

For Foreign Currency (FC) Exchange:

- **If the amount is AED 1 to 3500, FLAs will ask for the ID and verify if the same customer. They will record basic information such as below in the system and they will process the transaction. All customers will be recorded regardless amount and will get UIN in order to screen them.**

  a) Full legal name;
  b) Residential status (whether UAE Resident or UAE Non-Resident);
  c) Mobile number;
  d) Nationality;
  e) ID type (whether Emirates ID or Passport or GCC national ID); and
  f) ID number.

- **If the amount is AED 3,500 to AED 34,999.75, FLAs will perform CDD. That is, they will collect valid ID and photocopy and upload in the system. Also, they will attach in the vouchers. Information will be gathered and put in the system such as below:**

  a) Full legal name;
  b) Residential status (whether UAE Resident or UAE Non-Resident);
  c) Address in the UAE (for UAE Residents);
  d) Temporary address in the UAE and the permanent address in the home country (for UAE Non-Residents);
  e) Mobile number;
  f) Email, if available;
  g) Date of Birth;
  h) Nationality;
  i) Country of Birth;
  j) ID type (whether Emirates ID or Passport or GCC national ID);
  k) ID number;
  l) ID place of issue;
  m) ID issue date;
  n) ID expiry date;
  o) Profession; and
  p) Expected annual activity (i.e., expected annual value and number of transactions for future transaction monitoring).

- **If the amount is AED 55,000.00 and above (one time or within 90 days), FLAs will perform EDD. That is, they collect valid ID, verify, upload in the system, attach the ID in the voucher and collect pertinent**

supporting documents like Bank Withdrawal Slip, Bank Statements, Invoice, Bill of Lading and etc. Then, information above will be noted in the system.

For Remittance:

- If the amount is AED 1.00- AED 54,999.75, FLAs will perform CDD. That is, they will collect valid ID and photocopy and upload in the system. Also, they will attach in the vouchers. Information will be gathered and put in the system such as below:

  a) Full legal name;
  b) Residential status (whether UAE Resident or UAE Non-Resident);
  c) Address in the UAE (for UAE Residents);
  d) Temporary address in the UAE and the permanent address in the home country (for UAE Non-Residents);
  e) Mobile number;
  f) Email, if available;
  g) Date of Birth;
  h) Nationality;
  i) Country of Birth;
  j) ID type (whether Emirates ID or Passport or GCC national ID);
  k) ID number;
  l) ID place of issue;
  m) ID issue date;
  n) ID expiry date;
  o) Profession; and
  p) Expected annual activity (i.e., expected annual value and number of transactions for future transaction monitoring).

- If the amount is AED 55,000.00 and above (one time or within 45 days), FLAs will perform EDD. That is, they collect valid ID, verify, upload in the system, attach the ID in the voucher and collect pertinent supporting documents like Bank Withdrawal Slip, Bank Statements, Invoice, Bill of Lading and etc. Then, information above will be noted in the system.

PEP/FPEP CUSTOMERS:

In Al Dhahery Money Exchange, PEP/FPEP customers are automatically considered High Risk Customer. If the PEP/FPEP customer comes in to the branch, FLA informs Compliance Department before they can register the customer. Compliance will check whether customer has adverse media or none. If the PEP/FPEP customer has no adverse media, the Compliance Department will send approval request to the Owner. Once approved, FLA can proceed to register and execute transaction following KYC process. If the customer has adverse media, Compliance will advise FLA to not proceed with the registration and just advise that person that the company is facing system glitch and he could not proceed with the registration and transaction. If it merits reporting to authority, ADME will do so.

CORPORATE CUSTOMERS:

For Corporate customers, regardless of risk ratings, ADME applies EDD KYC process. FLA cannot process transaction if the corporate customer is not registered. Before registering the corporate account, KYC documents are collected and verified. Manual Sanctions screenings are performed. Site Visit is done as well. Approval from Compliance Officer and General Manager are taken before the registration. If one of the stakeholders is PEP/FPEP, approval from the Owner is needed before it can be registered.

In the event valid IDs of authorized representatives and trade license of the corporate customers are expired, FLA will be alerted by the system and FLA will inform Compliance Department.

Periodic/Annual EDD update is being done by Compliance Department to help FLA to execute transactions properly. All pertinent supporting documents (Bank statements, Bank Withdrawal Slip, Invoice, Bill of Lading, etc..) are collected as part of EDD process. EDD is also repeated whenever there is a change in the profile such as ownership change of the legal person. (Related paragraph in the standard chapter 16 (16.11.2 and 16.11.7 b, c.).

ADME Transaction Monitoring

Transaction Monitoring refers to the monitoring of customer transactions, including assessing historical/current customer information and interactions to provide a complete picture of customer activity. This can include transfers, deposits, and payments, foreign currency exchange.

ADME monitors all the transactions for detecting any unusual/ suspicious activity based on ongoing transactions (both real time and post transaction) for all products and services using a Risk-Based Approach.

Objective

- **The objective of TMS policy is to secure the financial institution from financial Crimes.**
- **Ensure that all transactions conducted are in compliance with its policies and procedures and the local and international regulatory framework.**
- **Scrutinize all transactions and assess whether they are in line with the customer's risk profile or known business activity.**
- **Re-assess the risks associated with the customer, product, or service as appropriate.**
- **Identify unusual or suspicious transactions that may ultimately require the ISTR filing.**
- **Strengthen its KYC and CDD procedures.**

Transaction Approval or Reject.

Transaction maybe rejected if it violates ADME Rules incorporated in TMS by the compliance team.

SYMEX TRAX- Automated System

ADME is using SYMEX TRAX advanced automated tool for day-to-day transaction monitoring efficiency. TMS is adequate with respect to its size, activities and complexity and the risks present, analyze trends in a single or a set of transactions and to identify unusual or suspicious transaction.

SYMEX TRAX is able to identify many cases of AML, Fraud or Sanctions Related cases based on various rules and scenarios inbuilt within the system. Transactions which fall under such rules or scenarios are then placed

in queue for further analysis by the Compliance Department in ADME. All such cases require Disposition remarks by the maker who analyses the transaction and such remarks are then verified, closed or reverted by the checker.

Live Rule Parameters

Rule Wise Report

ruleNumber	ruleName	service
1	1 - One customer sending funds to multiple beneficiaries in a set period (One Month Period)	Outward Remittances
2	2 - One customer receiving funds from multiple senders in a set period (one Month)	Inward Remittances
3	3 - Any transaction greater than the set threshold amount done by Individual	ALL
4	4 - Customers sending/receiving funds more than the set threshold in the last one month Individual	Inward/Outward Remittances
5	5 - Customer Sending more than 5 transactions in a set period individual	Outward Remittances
6	6 - Transaction made to high risk countries	Outward Remittances
7	7 - Transaction received from high risk countries	Inward Remittances
8	8 - Transactions more than a X amount done by high risk nationalities(AED 1 or above)	ALL
9	9 - No of Transactions performed in current month compared to last 3 months if exceeds X %	ALL
10	10 - Customer performing transactions in multiple branches in a set period	ALL
11	11 - Customers who are sending funds to same beneficiary more than 3 times in a month	Outward Remittances
12	12 - PEP customer transactions	ALL
13	13 - Same mobile Number used for more than one customer	ALL
14	14 -DNFBPs/DPMS customer transactions	FCY
15	15 - Same Sender sending funds to more than one beneficiary (WEEKLY)	Outward Remittances
16	16 - Customer sending funds to any other country than his Nationality	Outward Remittances
17	17 - Customer receiving funds from any other country than his Nationality	Inward Remittances
18	18 - Customer sending funds to any beneficiary other than his nationality	Outward Remittances
19	19 - Customer receiving funds from any beneficiary other than his nationality	Inward Remittances

20	20 - Customers sending funds to multiple countries in a set period	Outward Remittances
21	21 - Customers receiving funds from multiple countries in a set period	Inward Remittances
22	22 - Remitter/Beneficiaries name which can be identified as institutions for Charity, Social and Religious Organizations Customer sending funds to social organizations	Outward Remittances
23	23 - Watch list customers	ALL
24	24 - Employee threshold	ALL
25	25 - Foreign currency exchange transactions of aggregate value upto AED 34,999.75 per week	FCY
26	26 - Customers sending/receiving funds more than the set threshold in the last 7 days Corporate	Inward/Outward Remittances
27	27 - Customer Sending more than 5 transactions period for one month	Outward Remittances
28	28 - High risk Customer Manual Risk	ALL
29	29 -Corporate Customer performing any transaction in Cash	Outward Remittances
30	30 -Customers sending funds to multiple nationalities in a set period	Outward Remittances
31	31 - Customers receiving funds to multiple nationalities in a set period	Inward Remittances
32	32 - Money transfer transaction of aggregate value upto AED 27,000 per week	Outward Remittances
33	33 - High risk nationality send/receive funds from other nationalities	Inward/Outward Remittances
34	34 - High risk transaction	ALL
35	35 - Suspicious-word Check	ALL
36	36-Transactions more than AED 55000 in 45 days	Inward/Outward Remittances
37	37 - FC Exchange transaction value equal to or above AED 55,000 IN 90 DAYS	FCY
38	38 Customer marked in case violation	ALL
39	39 Non registered customer doing transaction Above than 3500	ALL
40	40-Expired kyc of the customer	ALL
41	41- Customer with same name or same Identity number should be registered	ALL
42	42-occasional transaction in the form of wire transfer for amounts equal to or exceeding AED 3500	Inward/Outward Remittances
43	43-FC/REMITTANCE transaction value equal to or above AED 55,000	ALL
44	44 - FC Sales Transaction >5000 AED	FCY

45	45- FC Purchase > 15000	ALL
75	75 - Transactions done using Seaman ID in one week and amount of FCY > 34999.75	FCY
76	76 - Transactions done using Seaman ID in one week and amount of Inward/Outward > 27000	Inward/Outward Remittances
46	46 - Case Management	ALL
47	47- Individual customer exchanging multiple currencies	ALL
77	77-FC transactions more than 2 in a month	ALL
78	78 - Transaction amount exceeds expected annual Activity	ALL

Risk Based Approach TMS Measures

ADME adopts a risk-based approach to transaction monitoring, which must include the following components:

- **Scrutiny of customer transactions to ensure that the transactions are in line with the knowledge of the customer, his business, risk profile, source of wealth and funds.**
- **Review of customer records to ensure that documents, data and information collected during the KYC, CDD and monitoring processes are relevant and up to date.**
- **Ideally performing transaction monitoring on the real time basis, to ascertain whether there has been any breach of rules or whether there is suspicion regarding a particular transaction.**
- **Using the information collected during the onboarding process that is related to the customer 's expected annual activity in order to assess any deviations or identify unusual patterns.**
- **Investigating any unusual or suspicious transactions and maintain all supporting records for a minimum period of 5 years.**
- **Following the investigation of unusual transactions, if there are reasonable grounds for suspicion, The Compliance Officer must immediately report such transactions to the FIU through GOAML.**
- **The Compliance Officer must retain documentary evidence with the reasons as to why any unusual transactions were not reported to the FIU.**
- **Configuring its monitoring system by defining a sufficient number of rules and parameters in the system so as to effectively identify unusual or suspicious transactions, patterns of activities or customer behaviors.**
- **Using parameters that reflect and take into account its risk assessment and profile.**
- **Using parameters tailored for both natural persons and legal entities so as to cater for the different types of transactions effected.**

Alert generation: alerts are generated based on the pre-defined rules/ scenarios built in the system.

Alert Investigation & Escalation: All alerts generated are then analyzed and investigated by the Compliance team and if necessary, alert is then escalated to Compliance Officer through Case Management System in Symex Trax.

Identifying suspicious activities: All transactions which are deemed to be suspicious are then escalated for potential reporting of STRs.

Real-time notifications and alerts are based on the below defined rules. Some of the logics mentioned below (list not exhaustive)

Escalation process of transactions and queries

In ADME the escalation process when an Employee suspects a transaction to be unusual / suspicious could be summarized as follows:

- **Escalate suspicion to the Compliance department internally via email.**
- **Upon receipt of the report from the staff, the Compliance Officer shall verify and do further investigation, EDD on the transactions etc.**
- **Escalation happens automatically through the system (system used by the exchange).**
- **When there is any suspicious activity or transaction identified through rule alert than case is created in case management for future monitoring and escalated by ACO to CO for review and approval.**
- **Mark the customer as high risk and should conduct an EDD for future transactions However, the compliance officer can block the customer for future transactions based on the severity of the issue**
- **Come up with the decision whether it should be reported (STR) to the Central Bank of the U.A.E or not.**

Reporting of Unusual / Suspicious Transactions through ISTR's:

It is the duty of all FLA's and officers to report suspicious and unusual transactions to the Compliance Officer who is the designated MLRO.

When potentially suspicious transactions are identified by a member of staff, they should be immediately reported to Compliance department through the ISTR form. The CO/ACO will perform an investigation and if confirmed as suspicious, then the case will be reported to FIU in the form of a Suspicious Transaction Report (STR)/ Suspicious Activity Report through GOAML Platform.

The compliance team shall maintain records relating to ISTRs and STRs, including the customer and transaction information and details of any action taken as a consequence. The CO shall also maintain a register for recording STRs.

Failure to report suspicious and unusual transaction to the Compliance Department shall attract disciplinary action.

Reporting and filing of STR's/SAR's:

This policy mandates the investigation of all alerts that may be suspicious and document the steps taken in the investigation in the form of an Internal Suspicious Transaction Report ("ISTR").

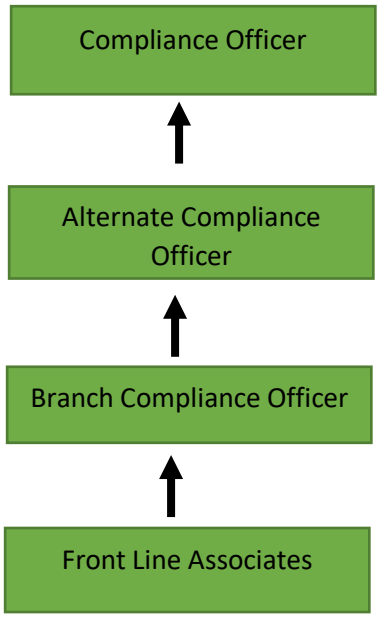
Compliance Officer - determines whether a Suspicious Transaction Report ("STR") is necessary based on the findings. Once, decision has been made to proceed with an STR, Compliance Officer is responsible to raise an STR to the FIU of the Central bank of UAE to notify the activity / transaction through GOAML platform.

STR shall be filed

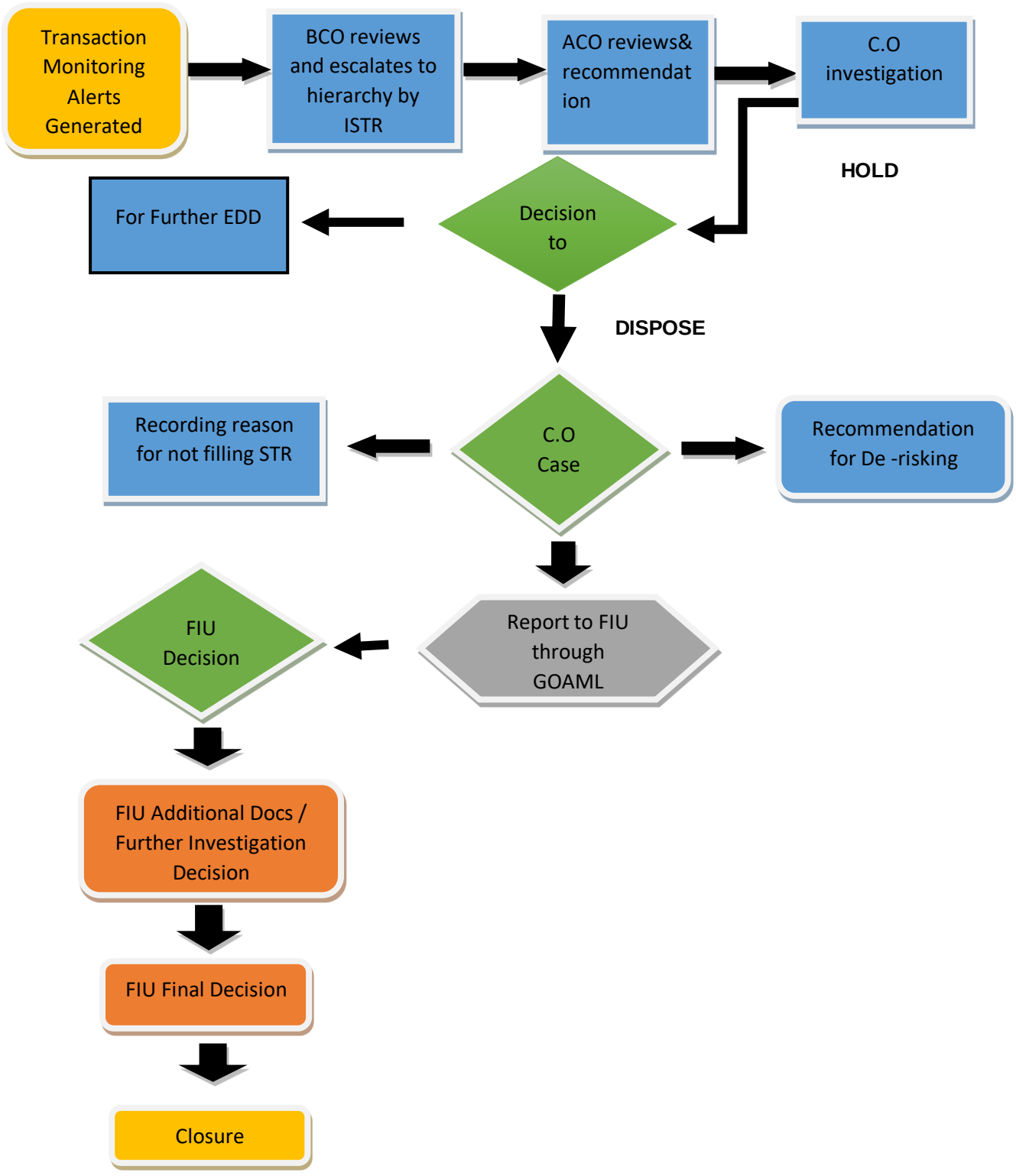
- **If further investigation is required and the suspect is unknown STR must be filed on detection of the suspicious activity.**
- **Even if the transaction is not reported, the Compliance Officer shall set forth the findings in writing and the same shall be retained.**
- **The Compliance Department shall maintain a register for recording the Suspicious Transaction Reports made to or by the Compliance Officer. The same shall be retained for unspecific period with the records of any action taken.**
- **Failure to report suspicious/unusual/attempted transactions shall attract legal and disciplinary action.**

- **By ignoring key indicators on Money laundering/ Terrorist Financing, an employee is considered to have directly partaken in such an activity through "willful blindness".**
- **In case a suspicious activity is identified against a payment or an inward remittance, the Compliance Officer may decide to seek appropriate permissions from the Central Bank of the UAE to freeze such funds. CBUAE shall be informed in case the transfer is not received and returned to the customer. In case the Central Bank issues directions to freeze the funds, the same should be for a period not exceeding 7 working days. Upon freezing the funds, the customer should be notified of the decision with instructions to provide the relevant documentation to ascertain the soundness of the transaction.**
- **All relevant details of any internal and external STR shall be kept in safe custody of Compliance department.**

ALERT Escalation Team:



The Escalation Process Flow:



Post STR and SAR Process

ADME has exit and retaining policy for all reported STRs and SARs. All the customer and business relationship reported to FIU is classified as HIGH-RISK customer and appropriate RBA based EDD and ongoing monitoring procedure is implemented to mitigate the associate ML/FT.

ADME also place the customers into internal watchlist and case management for monitoring purposes. Any Name on the list requires clearance from compliance team to execute the transaction. Furthermore, unless it is instructed by the FIU Al Dhahery Money Exchange documented plan for retaining or exiting the relationship.

ADME may decide to maintain the relationship of a customer, it will document the process of decision based on the condition related to and will implement adequate EDD measures to manage the account and mitigate the risk of ML/FT. Addition to that ADME will collect more data, documents from the customer in order to carry out transactions with Dual approval process. ADME will make sure to follow inline with Notice 3354/2022 STR Guidelines for Exchange Houses.

Typology and Red Flag Indicator

Typology	Red Flag Indicators
Structuring	Many transactions conducted at various financial institutions and/or branches, in one day. Small/frequent cash deposits, withdrawals, electronic transfers made over a short period. Multiple low value domestic or international transfer.
Smurfing	Third parties conducting numerous transactions on behalf of other people. Many transactions conducted at various financial institutions and/or branches, in one day.
Co-Mingling	Significant and/or frequent cash transactions when business has electronic funds transfer at point-of-sale facilities. Large number of accounts held by a customer with the same financial institution. Accounts operated by someone other than the account holder. Merging businesses to create layers. Complex ownership structures. Regular use of third-party accounts.
Unusual High Value Transactions	High value of cash transactions. Transaction does not match with the customer's profile or the entity's economic activity. Unusual transaction behaviour compares to customers with similar profiles.
Sudden increase in the turnover	Sudden increase in the value or annual turnover without an apparent reason. Unusual/high turnover from corporate clients and exchange houses, in contrast with others.
Cash exchanges - Refining	Significant and/or frequent cash exchanges from small to large denominations (refining).
Currency conversion	Significant and/or frequent local or foreign currency exchanges. Opening of foreign currency accounts with no apparent business or economic purpose.
Fraudulent Transaction Receipt	Representative of Corporate Entity/Exchange House/Individuals used fabricated transaction receipts to exchange illegal foreign currency.

Cash couriers	Transactions involving locations with poor AML/CFT regimes or high exposure to corruption. Customers originating from locations with poor AML/CFT regimes/high exposure to corruption. Significant and/or frequent cash deposits made over a short period of time. Significant and/or frequent currency exchanges made over a short period of time.
Carrying large value of foreign currency	Representative/employee of exchange house carried large volume of banknotes by hand to an exchange house.
Purchase of valuable commodities	Significant and/or frequent cash purchases of valuable commodities. Regular buying and selling of valuable commodities that does not make economic sense.
Sudden increase in turnover from one branch	Volume/Turnover of transactions has been increased from one particular exchange house.
High Value or change in salary (WPS) transactions to employee	High value salary transaction to employees. Change in salary amounts, compared to previous months.
Numerous remittances to same or different beneficiaries	Customers sending money to same or different beneficiaries.
Receiving money from many senders	A customer is the beneficiary of a high number of remittances (often in relatively small amounts) during a short time.
Purchase of valuable assets	Purchase/sale of real estate above/below market value irrespective of economic disadvantage. Cash purchases of valuable assets with cash and/or cash deposits for valuable assets. Low value property purchased with improvements paid for in cash before reselling. Rapid repayment of loans/mortgages with cash or funds from an unlikely source.
Remittance to/from High-Risk Countries	Transfers to countries that have weak AML controls or high exposure to corruption. Transfers to high-risk countries or tax havens.
Large Cash Deposits	High value of transactions by paying cash to introduce illegal money into financial system.
Frequent Currency conversion	Frequent local or foreign currency exchange in short period of time, without an apparent reason.
Corruption through publicly exposed Persons	Use of Corporate companies and Domestic Financial Institutions to launder money
Transactions inconsistent with intended purpose	Transactions to and from unrelated parties. Transaction amounts, which are abnormal to the account's expected volumes, amount, or frequencies. Transactions, which are out of line of the customer's profession or business activity. High value of transactions, that do not match the client profile.

Underground banking/alternative remittance services	Mostly prevalent under the garb of a general trading company license. Significant and/or frequent cash payments for transfers in which the cash deposits could be from many different individuals using the cash deposit machines Cash volumes and transfers in excess of average income of migrant account holders. Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption. Large transfers from accounts to potential cash pooling accounts. Significant and/or frequent transfers recorded informally using unconventional book-keeping. Significant and/or frequent transfers requested by unknown or intermittent customers. Numerous deposits to one account followed by numerous payments made to various people. Vague invoices and documentation which may deliberately be made to appear complex
Gatekeepers/professional services	Accounts and/or facilities opened and/or operated by company formation agents. Gatekeepers that appear to have full control. Known or suspected corrupt professionals offering services to criminal entities. Accounts operated by someone other than the account holder.
Wire transfers to and from bank accounts	Significant and/or frequent cash payments for transfers. Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption. Transfers to high-risk countries or known tax havens. Transfers to numerous offshore jurisdictions with no business rationale. Same home address provided by multiple remitters. Reluctant to provide retailer with identification details
Nominees, trustees, family members or third Parties	Customers using family members or third parties, including the use of children's accounts. Transactions where third parties seem to be retaining a portion of funds (i.e., Mules). Accounts operated by someone other than the account holder. Many transactions conducted at various financial institutions and/or branches, in one day. Significant and/or frequent transactions made over a short period of time.

Trade Based Money Laundering (TBML)	**Over-invoicing:** By invoicing the goods or service at a price above the fair market price, the seller is able to receive value from the buyer, as the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market. **Under-invoicing:** By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer, as the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market. **Over-shipping or Short-shipping:** A mismatch in the invoiced quantity of goods and the quantity of goods in fact shipped. By over or under-shipping, the invoiced quantity of the goods, the buyer or seller (as the case may be) gains excess value when the payment is made. **Fictitious Trades or Phantom shipping:** A seller may not ship any goods at all, but simply collude with a buyer to ensure that all shipping and customs documents associated with the trade. Also known as "ghost shipping" or "phantom shipping". **Multiple Invoicing of Goods and Services:** Issuing more than one invoice for the same trade transaction. By invoicing the same goods or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. **Use of Shell or Fictitious Companies:** A shell corporation is a non-traded corporation without any active business operations. They can be set up in a matter of days with minimal time and paperwork. They typically have little or no revenue and very few assets, and many of them don't even have a physical location. Shell companies are often the vehicle behind tax evasion, money laundering, bankruptcy fraud, market manipulation, and other various operational schemes. They typically leave no paper trail because they have no tangible assets and can sometimes get away with submitting very little legal paperwork. The process of transforming money obtained from crime into money that appears to have come from legitimate sources. For example, a drug trafficker can launder dirty money through a shell company by declaring illegal drug proceeds as legal income through his or her "business," which is actually a shell company with no real operations. **Black Market Trades:** Commonly referred to as "black market peso exchange arrangements" (or similar), this usually involves the domestic transfer of funds (that need laundering) to pay for goods on behalf of a foreign importer.
Offshore companies	Large numbers of companies registered with the same office address. Address supplied is a 'Virtual office'. Accounts/facilities opened/operated by company formation agents. Lack of information regarding overseas directors/beneficiaries. Complex ownership structures. Structures where there is no apparent legitimate economic or other rational. The same natural person is the director of a large number of single director companies.

	The same person (natural or corporate) is the shareholder of a large number of single-shareholder companies.

General indicators

In addition, any of these red-flag indicators, in conjunction with shipments to duty-free zones of high dollar merchandise such as electronics, auto parts, precious metals could be an indication of trade-based money laundering or BMPE activity. It is important to remember that no activity by itself is a clear indication of trade-based money laundering. Due to some similarities with legitimate financial activities, financial institutions should evaluate indicators of potential trade-based money laundering in combination with other red flags and expected transaction activity for its customer before making determinations of suspiciousness. Additional investigation and analysis may be necessary to determine if the activity is suspicious, based on information available to the financial institution.

Typologies used by the Individual Customers
▪ Organized crime and narcotics-traffickers ▪ Money Laundering Through the Physical Transportation of Cash ▪ Importation of high foreign currency and traveller's checks not commensurate with stated occupation ▪ Abrupt change in pattern of Activity. ▪ Movement of funds through countries that are on the FATF list of NCCTs. ▪ Terrorist Activity ▪ No known source of income ▪ Use of wire transfers and the Internet to move funds to and from high-risk countries and geographic locations. ▪ Purchases of military items or technology ▪ Currency Exchange Without any apparent purpose ▪ Alternative Remittance Systems

Typologies used by the Corporate Customers
▪ Organized crime and narcotics-traffickers ▪ Financial activity inconsistent with the stated purpose of the business ▪ Money Laundering Through the Physical Transportation of Cash ▪ Importation of huge foreign currency not commensurate with stated occupation ▪ Paying out fictitious salaries ▪ No apparent business relationship between the parties and transactions ▪ Lack of appropriate documentation to support transactions. ▪ Abrupt change in pattern of Activity. ▪ Movement of funds through countries that are on the FATF list of NCCTs. ▪ Apparent use of personal profile for business purposes ▪ Use of multiple Customer profile personal and business accounts to receive and then funnel funds to a small number of foreign beneficiaries. ▪ Use of possible shell companies ▪ Over Invoicing for a Trade Transaction

- Multiple Invoicing
- Chance of employee fraud during currency purchase transactions between financial institutions. (Fake bills)
- Terrorist Activity
- No known source of income
- Use of wire transfers and the Internet to move funds to and from high-risk countries and geographic locations.
- Purchases of military items or technology
- The use of funds by non-profit organization is not consistent with the purpose for which it was established.
- Fund Transfers Without any apparent purpose
- Alternative Remittance Systems

Red Flag Indicators based on Notice 3354/2022:

- No supporting documentation in relation to the origin or owner
- Customer is suspected to be working or acting on behalf of, or is controlled by, a sanctioned individual, group, or entity.
- Pattern of transactions has changed since business relationship was established.
- Transactions or series of transactions that appear to be unnecessarily complex, that do not have a discernible economic rationale.
- Numbers, sizes, or types of transactions that appear to be inconsistent with the customer's expected activity.
- Transaction from restricted countries or owners of restricted countries, or countries with a high level of corruption or political instability
- No explanation given for the receipt of the funds, incomplete, unlikely, or partly incorrect explanation.
- Transaction is suspected of being linked (directly or indirectly) to nuclear weapons Programme.
- Customer suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.
- Use of missing/suspicious/falsified documents, e.g.: ID, Invoice or Bill of lading is or seems to be forged.
- Customer works as a labourer wishes to transfer a sum that is greater than the average yearly income and doing for someone in his position.
- Customer visits the company on a regular basis and makes small or moderate-sized transfers, but the sum of the amounts he transfers over the course of the year is greater than the yearly income for someone in his position.
- Customer has no occupation but continues to make transfers or transfers a large sum.
- Customer is from country A and wanted to send/receive funds to a family member, but beneficiary located in country B.
- Customer makes regular transfers from country A to family members, but the members live in different region in country A and their relationship to the customer is not clear.

Validation of typologies

The identified typologies are then validated through internal review of existing rules and rule violation lists of the Exchange House.

Develop controls and Rule Optimization

Once the typologies have been validated, the Exchange House must fine tune the existing rules to mitigate the risks associated with these typologies. The implementation of optimised rules enhances the overall AML program.

Potential Risk Indicators relevant to Exchange House based on the updated Typology

- **Sudden increase in the value or annual turnover without apparent reason**
- **Increased turnover from one particular branch of exchange house**
- **Representative of exchange house uses fabricated transaction receipt to exchange illegal foreign currency**
- **Employees of the exchange house were directly carrying large volume of banknotes to the exchange house instead of using CIT companies**
- **Unusual/high turnover from a particular exchange house in contrast to others with similar business Models**
- **Exchange houses selling in high values of a single foreign currency**

Tipping off

ADME policy governs that staff of ADME shall not warn or share the information with the concerned individual and/or entity about the information being reported to/investigated by the relevant authority. Any deviation to these guidelines shall attract disciplinary action.

All staff should note that he/she must not inform any customer/colleague that the customer is being scrutinized for possible involvement in suspicious activity related to money laundering, or that a competent authority is investigating his possible involvement in suspicious activity relating to money laundering.

If the employee reasonably believes that performing CDD will tip-off a customer or potential customer, employee may choose not to pursue that process. If the employee decides to do so then he/she must promptly notify the CO/ALCO, who will decide whether an SAR should be filed. When reporting suspicious transactions to the FIU, FIs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT Sanction framework, and in keeping with the nature and size of their businesses, FIs, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organization. It should be noted that the confidentiality requirement does not pertain to communication within the supervised institution or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to ML/FT. It is a federal crime for FIs or their managers, employees or representatives, to inform a customer or any other person, whether directly or indirectly, that a report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction

Penalty of Tipping Off

According to the Federal Decree Law no (20) of 2018 Article 25 Any person violating this rule and regulation shall face Imprisonment for no less than six months and a penalty of no less than AED 100,000 (one hundred thousand dirham) and no more than AED 500,000 (five hundred thousand dirham) or any of these two sanctions shall apply to anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated by the Competent Authorities.

ADME Adherence for KYE

Human Resources (HR) function plays a key role in hiring and retaining people with integrity, professionalism and the appropriate set of knowledge, skills and competences for the company. Employees are the foundation and the face of ADME and it is therefore of utmost importance that there is a strong and effective Know Your Employee (KYE) policy in place.

The main objective of this policy is to know the background of applicants prior to placing them in employment, to uphold the values and principles of ADME and mitigate the risk of fraudulent action.

Know Your Employee Guidelines: Pre-Employment

ADME shall implement an appropriate recruitment process and KYE policy that must include the following at a minimum:

- **Screening of CV.**
- **UAEPNG checking.**
- **Verification of applicant's academic qualifications.**
    - **Testing and interview process.**
- **Employment history verification. This could be performed by obtaining a letter from the previous employer(s) and by contacting the latter to confirm the employee's work experience and to gather information on previous role(s). Such information could include: Duration of employment.**

Employment credentials such as designation, role, key tasks and responsibilities.

- **Conduct during the employee's tenure.**
- **Reason for leaving.**
- **Checking of references, either with the same company itself or by an outsourced agency. Referees provided by the prospective employee should be requested to provide further information on the details stated by the applicant on the CV or job application.**
- **Police Clearance Certification from the police authority if each respective emirates (if the employee is already in UAE or Police Clearance Certification from the home country).**

Sanctions screening checks.

In addition to pre-employment background checks, it is advisable to perform random checks during the course of employment so as to mitigate potential internal threats to the business. ADME shall watch out for warning signs in their employees' conduct and behavior that could be red flags for fraud.

Warning Signs

Circumventing: Employee frequently overrides internal controls or established approval authority or circumvents policy.

Behavior: a change in the employee's lifestyle that cannot be explained by the salary or other change in the individual's financial circumstances (e.g., inheritance) as well as employees who are reluctant to take a vacation or is associate with an unusual large number of transactions.

Loans: frequent requests for loans should be carefully scrutinized.

Overzealous relationship with select customers: there have been instances where customers have offered bribes and commissions to employees of financial institutions in return for assistance with conducting fraud, embezzlement and money laundering. Frequent checks and controls on the activities of employees can help detect these activities at an early stage.

Timing: often employees in critical areas of operations and accounts have been caught for perpetrating internal fraud. These employees have been reported to have long working hours, coming in early and staying late. Also, they are often reluctant to take a vacation.

Transactions: an employee who is associated with an unusually large number of transactions compared to his peers.

Exaggerates Credentials:

Employee exaggerates the credentials and background to get more benefit from management.

Compromising data and system integrity: Employees who have often been reprimanded for misuse of confidential data and systems should be monitored closely for mitigating any risk of fraud.

Unresolved Exceptions

Employee is involved in an excessive number of unresolved exceptions, it's risky because it will damage the corporate culture in the company.

Using Company Resources

Employee uses company resources to further private interests.

More often than not there are simple explanations for certain behaviors, but it is sensible managerial practice to be alert to the possibility that those acting out of character could be up to no good. ADME shall implement a Code of Conduct to be signed by all employees upon joining the company. The Code must include the following at a minimum:

- **Guidelines for acceptable behavior.**
- **Mandatory policies, procedures and regulations.**
- **Confidentiality.**
- **Conflicts of interest.**
- **Disciplinary procedures.**
- **Right to appeal.**

Training

Employee training is one of the key pillars of an effective AML program and key to any financial institution's fight against money laundering and terrorist financing. ADME shall provide comprehensive AML/CFT training to all employees, including senior management and the Owner of Company.

To maintain an effective AML/CFT Sanction program in Al DHAHERY Money Exchange all our employees should be aware of this policy and trained to identify and report suspicious activity. For this purpose, the Compliance Officer or a third party provides all relevant employees with annual AML/CFT training.

Frequency

ADME shall provide AML/CFT training as follows:

- **New employees: induction training within 30 business days from joining.**
- **All employees: refresher training at regular intervals. ADME may determine the frequency of refresher training based on the risk exposure of the employee. However, employees who deal directly with customers, products and services must receive annual training at a minimum.**
- **All employees: refresher training whenever there are changes in AML/CFT laws or regulations; the Standards; or the policies and procedures of ADME.**
- **Owner training as per training schedule**

.

In AL DHAHERY Money Exchange, we ensure that the Compliance Officer and Alternate Compliance Officer other compliance staff must undergo a minimum of forty-eight (48) hours external training in AML/CFT Sanction compliance every year as a part of the Continuous Professional Development Program.

Training records

ADME shall maintain records and make them available to CBUAE examiners as follows:

- **Training registers in order to verify the training history of each employee.**
- **Training policy and plan.**
- **Training materials.**
- **Training schedules and employee sign-off forms.**
- **Employee assessment sheets and training certificates**

Agenda Items

- **Training to the Owner. (It is very vital part of ADME training and compliance team will give proper AML/CFT training to Owner and also keep her apprised with current regulatory laws and regulations).**
- **Senior Management Training**
- **AML/CFT Induction Training.**
- **TF PF Training.**
- **Fraud- Anti Fraud Induction Training**
- **New Updates on AML/CFT Laws & Regulatory Standards**
- **Introduction to Money Laundering - Money Laundering & Terror Financing**
- **Compliance Culture, Governance & Monitoring**
- **Risk Identification, Assessment, Mitigation & Risk Based Approach (RBA)**

- **KYC, CDD, EDD & Transaction Monitoring System (TMS) Training**
- **Suspicious Transactions, Processes and procedures of making internal disclosures of unusual transactions**
- **AML/CFT policies and procedures: Tipping Off, Record Retention Policy, Roles of CCO & ALCO & Laws, Regulations, Penalties, Notices and the Standards.**
- **Sanction Screening**
- **International guidelines FATF**
- **Anti-Fraud Training**
- **Counterfeit Currency**
- **Consumer data protection regulation.**
- **Compliant management handling.**

Assessment

Assessments are done periodically and those that do not achieve the desired results, undergo a refresher training.

Training Material

The Topics covered by AML/CFT training has been tailored as per the roles of the employees, like senior management vs a teller vs a back-office employee. The Training material incorporates all the requirements of CBUAE.

Delivery Channels

At Al DHAHERY Money Exchange different channels are used for imparting AML/CFT Compliance Trainings. The channels are:

a. **Onsite training for new joiners: New Joiner is given a briefing about the systems and basic KYC check and AML/CFT sanction procedures of the company**
b. **Training Sessions (Meetings)**
c. **Inter Office Communications**
d. **Circulars**
e. **Through Email communications**
f. **E- learning modules like web based**

Training Register

The Compliance Team will maintain record of attendance of all conducted training sessions. Our Training register covers the following details:

- **Name of attendances, Designations, Branch details, DOJ (Date of joining)**
- **Attendance date**
- **Training date**
- **Agenda details**
- **Topic**
- **Training scores**
- **Fit and Proper test**
- **Upcoming scheduled events**
- **Senior management / Owner training schedule**

Independent Testing

The effectiveness to the AML/CFT Compliance program is assessed through the independent testing of Internal and external audit function.

A robust AML compliance program is deemed complete when it includes the requirement for an independent, regular review to be performed to assess the adequacy of the policies and procedures, systems and controls and the Compliance Officer's function. To review and test whether the AML function, policies, procedures and controls are in line with CBUAE requirements and recommend appropriate changes so that ADME may enhance its framework and make its controls more effective in the fight against money laundering and terrorist financing. Both internal and external audits play an important role in evaluating the AML/CFT framework of ADME In order to ensure that its AML compliance program is effective and adequate in assisting it to meet its regulatory obligations, ADME shall arrange for the following independent testing:

Internal Audit

SPARK MANAGEMENT CONSULTANCY FZE.
WE MAKE IT HAPPEN

***ADME has its outsourced internal auditor* SPARK Management Consultancy FZE**

who check the AML/CFT effectiveness across the branches and the Compliance department on a periodic basis. The audit reports of the branches are shared with the Operations & Compliance teams for improvement or corrective action if any.

- **Being as 3rd Line of Defense, the internal audit must be conducted on a regular basis, rely, and include the review of the organization's AML function and AML/CFT policies, procedures, processes and controls by use of a well-defined audit program.**

The internal and external auditors must issue reports encompassing any deviations identified, areas for improvement and suggested remedial actions as follows:

Internal audit report: directly to the Board of Directors.

External Audit

ADME has appointed External auditor Vertex Compliance (Agreed upon procedures) as per regulatory guidelines.

External Audit Report: is reported to the Owner for ensuring that the report is further submitted to the Banking Supervision Department of the CBUAE by 30 April each financial year

List of Compulsory Reports and Forms Prudential reporting and submission deadlines

ADME must submit the following returns/reports to the Central Bank within the deadlines mentioned hereunder:

No.	Name of the Return/Report	Frequency	Deadline	Submitted to
1	Daily Remittance Data - via Daily Remittances Reporting Systems of the Central Bank	Daily	Before the end of next business day	FIU via online systems
2	Bi-Annual Compliance Report from the Compliance	Bi-Annual /Semi MLRO	Within four months from the	BSD and FIU

	Officer as per Paragraph 16.30 of Chapter 16		end of the reporting period	
3	Submission of Auditors' Report, Financial Statements and Management Letter as per Paragraphs 7.3.4 (a) and 7.3.5 (d) of Chapter 7	Annual	On or before 31st March of the year following the end of the reporting period	BSD
4	Submission of External Auditor's findings based on the Agreed-Upon Procedures on AML/CFT Compliance function as per Paragraph 16.31.2 of Chapter 16	Annual	On or before 30th April of the year following the end of the reporting period	BSD

Notes:

1. **Annual return/report - reports for the period from 1st January to 31st December of each financial year.**
2. **Bi-Annual/Semi MLRO report - reports for the six (6) months period January ending on 30th June and July ending on 31st December of each financial year. It will cover policy procedures and internal controls.**
   A copy of Bi Annual/Semi MLRO Compliance Report must be submitted to the BSD and the AML/CFT Supervision department via email respectively to info.ehs@cbuae.gov.ae and amlcft@cbuae.gov.ae along with the comments from the owner within four months from the end of each reporting period.
3. **Quarterly reports - reports for the three (3) months period ending on 31st March, 30th June, 30th September and 31st December of each financial year.**
   In the case of a startup business, the starting date of a return/report will be the actual date of commencement of business in all above cases.
4. **Auditors' Report, Financial Statements, Management Letter and External Auditor's findings based on the Agreed-Upon Procedures on AML/CFT Compliance function (i.e., items 3 and 4 of the above table) must be submitted to the Banking Supervision Department via email info.ehs@cbuae.gov.ae in addition to submitting the hard copies.**

Daily Remittance Data

ADME RRS is automated upload from the core system to CBUAE managed site every 15 seconds and cross checked at the end of the day. If any failure (NAK) the report is regenerated manually and uploaded to the site, before the end of the next business day.

CBUAE Queries

ADME will respond to queries from the Central Bank or other local authorities, such as search or freeze notices, IEMS queries.

Anti-Fraud Framework

ADME considers Definition of the term 'fraud' as commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. Fraud essentially involves using trick to dishonestly make a personal gain for oneself and/or create a loss for another. Although definitions vary between offenders and victims. Frauds are broadly classified into Internal and External Frauds.

Core Objectives

- **Set the tone from top: ADME top level message is very clear "Zero tolerance"**
- **Fraud risk must be understood for internal and external frauds.**
- **Stringent controls on complex areas.**
- **Screening of all employees**
- **Training to educate the team members for compliance.**

Methodology

ADME will apply reconciliation controls, system controls and whistleblowing policy. Investigation will be conducted through research, follow-ups and interviews.

Reporting Channel:

- **Immediate Reporting FIU**
- **Litigation Process covering insurance, claims, disciplinary actions etc.**
- **Monitoring**

Responsible Personnel:

Manager In-charge & Owner

Fraud Officer

ADME has fraud officer in the company who is responsible to minimize the risk of fraudster activities.

At ADME, the concept of a fraud incident refers to all incidents, allegations and suspicions where there has been, or could be, whether internal or external (e.g., perpetrated by customers, suppliers, or any other party), that impacts ADME, regardless of materiality.

We ensure that our employees duly perform their duty in reviewing the documents and discovering the evidence of any suspicious transaction, and in such instance should take the necessary procedures with respect to the transaction presuming its existence would entail legal obligations. Fraud Officer will coordinate with HR department for disciplinary action.

Ms. Margie Cabral
riskofficer@aldhaheryexchange.com
Tel: 04-221 3211
Ext: 408

Reporting fraud is critical:
It helps ADME educate customers and can give authorities information about the latest frauds in the marketplace. We work frequently with other FI's but it's important to note that our role is not law enforcement and there are inherent dangers in trying to catch criminals, to our customers and counterparts. ADME believes in to cooperate with law enforcement agencies at utmost priority to help in the investigation and prosecution of people who take advantage of our services to commit fraud.

ADME concerned about Scams

ADME is very much conscious about different behaviors of fraudster activities for money remittance products and conducting appropriate training sessions and applying strong controls to minimize these risks.

External Frauds: Fraud Committed by external party against the business.

Advanced Fee

Victim is asked to pay upfront fees for financial services which are never provided. Victims often send a succession of transactions for payment of various upfront fees. Common methods could include: credit card, grants, loans, inheritance, or investment

ADME team is watching such purpose of transactions very closely and following the regulatory guidelines.

Anti-Virus scam

ADME IT officer taking care of robust IT controls and no one is allowed to intervene in IT affairs without IT officer and committee approval, Team is only allowed to work with approved vendors only.

Victim is contacted by someone claiming they are from a well-known computer or software company and a virus has been detected on the victim's computer. The victim is advised that the virus can be removed and the computer protected for a small fee with a payment by either credit card or a money transfer. In reality, there was no virus on the computer and the victim has just lost the money they sent for the protection.

ADME all antivirus software are updated regularly and any unlicensed software is not allowed to incorporate into the system.

Charity Scam

IT team has applied controls on emails and any such emails are not accessible to our any staff member system.

The victim is often contacted by email, mail or phone by someone asking for a donation to be sent by money transfer to an individual to help victims of a recent current event, such as a disaster or emergency (such as a flood, cyclone, or earthquake). Legitimate charity organizations will never ask for donations to be sent to an individual through a money transfer service.

Emergency scam

Such Transactions are closely watched by FLA's and Compliance Personnel's. Team is well educated to mitigate risk of such frauds. Victim is led to believe that they are sending funds to assist a friend or loved one in urgent need. Victim sends the money with urgency as the victim's natural concern for a loved one is exploited; *Employment scam* Victim responds to a job posting and is hired for the fictitious job and sent a fake check for job related expenses. Check amount exceeds the victim's expenses and victim sends remaining funds back using a money transfer. The check bounces and the victim are responsible for the full amount.

Extortion

ADME team is well aware of human trafficking activities and compliance team not entertain such unusual requests and escalate it to next level for FIU's.

Threats to life, arrest or other demands by scammers to unlawfully obtain money, property or services from a victim through coercion that they supposedly owe and threatens if they do not cooperate.

Grandparent scam

ADME remittance staff well scrutinize such scams especially Emergency scam inn which the victim is contacted by an individual pretending to be a grandchild in distress, or a person of authority such as a medical professional, law enforcement officer, or attorney.

The fraudster describes an urgent situation or emergency (bail, medical expenses, emergency travel funds) involving the grandchild that requires a money transfer to be sent immediately. No emergency has occurred, and the victim who sent money to help their grandchild has lost their money.

E-Crime Frauds Understanding & Mitigation

ADME team is well educated to minimize the risks of E-Crimes and regulators are also educating to FI's regularly to apply robust and stringent model to minimize the risk of E-Crimes.

Identity Theft

Fraud officer/IT officer has made team aware for such identity theft frauds. Identity thieves use personal information (e.g., Social Security numbers, bank account information and credit card numbers) to pose as another individual. This may include opening a credit account, draining an existing account, filing tax returns or obtaining medical coverage.

Phishing

Communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the victim into providing personal information or passwords. A Phish is a fraudulent attempt, usually made through email (although can also be made via phone or text), to steal your personal information or propagate malicious code or software onto your computer.

Social Networking scam

If a cybercriminal gains access to your social media accounts, they also gain access to your close friends and family. Criminals and con artists can take advantage of how much personal information people share online, and then use this information to make skillful and highly targeted pitches to their friends and family, often involving requests for money.

SMS/Smishing

Beware of texts that spark urgency, asking you to click on a link, taking you to a compromised site, or get you to unwittingly divulge some personal information that could be used against you.

ADME Strategies for internal Fraud Prevention

Internal Frauds

ADME defines frauds committed by employed individuals.

Know Your Employees: **ADME understands Fraud perpetrators often display behavioral traits that can indicate the intention to commit fraud. Observing and listening to employees can help to identify potential fraud risk. It is important for management to be involved with their employees and take time to get to know them. Often, an attitude change can clue into a risk. This can also reveal internal issues that need to be addressed**

Set Up Reporting System: **ADME has policy that everyone within the organization should be aware of the fraud risk policy including types of fraud and the consequences associated with them. Those who are planning to commit fraud will know that management is watching and will hopefully be deterred by this. Honest employees who are not tempted to commit fraud will also be made aware of possible signs of fraud or theft. These employees are assets in the fight against fraud.**

Report, most occupational fraud is detected because of a tip. While most tips come from employees of the organization, other important sources of tips are customers, vendors, competitors, and acquaintances of the fraudster. Since many employees are hesitant to report incidents to their employers, consider setting up an anonymous reporting system. Employees can report fraudulent activity through a website keeping their identity safe or by using a tip hotline.

Implement Internal Controls

- **ADME Internal controls are the plans and/or programs implemented to safeguard for company's assets, ensure the integrity of its accounting records, and deter and detect fraud and theft.**
- **Segregation of duties is an important component of internal control that can reduce the risk of fraud from occurring.**

Documentation

ADME maintains strong documentary trail of all business transactions to minimize the risk of internal frauds. Our controls are monitored and revised on a consistent basis to ensure they are effective and current with technological and other advances.

ADME Fraud Register

ADME will maintain appropriate register to record the following information about fraud incidents and this register will be available for the verification by the auditors:

a) Date of fraud incident
b) Brief description of the fraud incident
c) Parties involved
d) Amount of loss
e) Was the loss covered by insurance or not?
f) Date of reporting to the police, FIU and the Banking Supervision Department
g) other actions taken and
h) Disciplinary actions taken, if applicable.

A review of Fraud Incident Register will be carried out at the end of every financial year to identify the anti-fraud training needs of employees for the following year.

Reporting Matrix

- **All fraud incidents must be submitted to police.**
- **Escalation to FIU**

- **Informing Banking Supervision department by using FIR form incase loss is equal or above 100,000 AED.**
- **50,000 AED equal or above must be reported to owners.**

Breaching Escalation Handling Policy

It covers the requirements for identifying, assessing, remediating, reporting and recording breaches of compliance obligations under the compliance policy.

IDENTIFICATION AND RESPONDING

- **All ADME staff who identify or suspect a breach must report it to their supervisor as soon as practicable. Evidence that may be valuable in determining the cause or allow for corrective action to be taken must not be compromised or destroyed.**
- **Managers must report the identified or suspected breach to the compliance department**
- **If staff are unable to discuss a breach with their supervisor, they must report the breach directly to the compliance department**
- **Staff who are aware of a breach and fail to report it may be subject to disciplinary action in accordance with the Code of Conduct.**
- **Where reasonable and practicable, immediate action must be taken to contain the breach.**

ASSESMENT AND MITIGATION

- **Compliance department are responsible for assessment of compliance breaches. The compliance department will assess the nature, scale and impact of breaches with reference to risk management protocols and determine the appropriate course of action.**
- **The assessment will identify root causes and determine whether the breach is an isolated or systemic issue. It will identify corrective or preventative actions to mitigate or eliminate the impact of the breach and likelihood of recurrence.**

REPORTING:

- **Suspected or actual breaches must be recorded**
- **Breaches relating to high-risk regulatory activities will be recorded by the compliance department**

CLIENT RETENTION:

Keep best knowledge of customer KYC is based on who is our customer's customer KYCC? This understanding enables us to establish strong relationship with our customer.

ADME believes in complete transparency with our existing and new customers. it maintains integrity and ethical values among our customers and keep them apprised with compliance guidelines.

Deviation of Procedure from Policy

It applies to all employees and persons in a comparable position, all departments, all branches in ADME, once adopted by Senior Management in case a policy conflicts with company stated requirements.

Approval: Senior Management can only approve a policy with deviations

Any material deviations from the policy must be reported to the Partners/Board of Directors of ADME. The aim of ADME is not only to comply with relevant legal requirements, but also to mitigates and reduce the potential risk to the company of our customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or perform transactions in breach of financial sanctions.

ADME Consumer Protection

ADME is adhering with establishment of Consumer Protection Department of Central Bank of UAE for aiming to protect consumers from financial misconduct through education, policy-making, and compliance monitoring and tracking of complaints resolution.

Owner of Program:

- **Owner of ADME**
- **Risk Officer**
- **General Manager**
- **Compliance Officer**
- **IT in-Charge**
- **Operation Manager**
- **Scope of Application**

ADME consumer protection covers the following scope:

- **Protect the consumer data with transparency and integrity.**
- **Maintain disclosure and transparency**
- **Management oversight**
- **Review and evaluate the market and business conduct**
- **Application of Financial standards**
- **Complaint management system and evaluation**
- **Training/education and awareness of consumer and employees**
- **Maintaining policy integrity and robust implementation**

ADME will maintain following standards:

- **Oversight: ADME will apply robust management oversight and responsibility structures in place for the activities including design, development, promotion, sales and distribution of products and/or services; compliance, risk and audit controls; up to date policies, procedures and training; engagement of qualified staff.**
- **Instill a Consumer- ADME will focused corporate culture that will treat consumers fairly. ADME must actively monitor, identify, respond and address misconduct and potential Market Conduct risks.**
- **Protection: ADME will ensure consumer financial assets; information and all data are secured and protected. The exchange should ensure security of these information at all cost.**
- **Governance: Strong governance and effective management oversight should be in place over the design, development, promotion, sales, distribution and the ongoing review and changes of Financial Products and/or Services.**
- **Effective Controls: ADME must have effective controls, strong security and monitoring of transactions and activities of staff. Compliance with the Regulation and accompanying Standard in retail activities through policies, procedures, training, systems and controls including and not limited to Complaint handling and Complaint resolution, Consumer education, compensation and practices in sales and advisory services.**

- **Transparency: The exchange is expected to maintain up to date policies and procedures, systems and controls that fully comply with the requirements specified within the Regulation and its accompanying Standards.**
- **Culture: Demonstrate a corporate culture of consumer service, fairness, transparency, ethical business conduct and effective disclosure.**
- **Confidentiality: With respect to Data confidentiality, ADME has its contractual rights in place to take legal action against the Service Provider in the event of breach of confidentiality.**
- **The Service Provider: must assure and ensure that the customer and transaction database are always held/stored within the UAE and kept confidential.**

ADME typologies for Data/Information Access

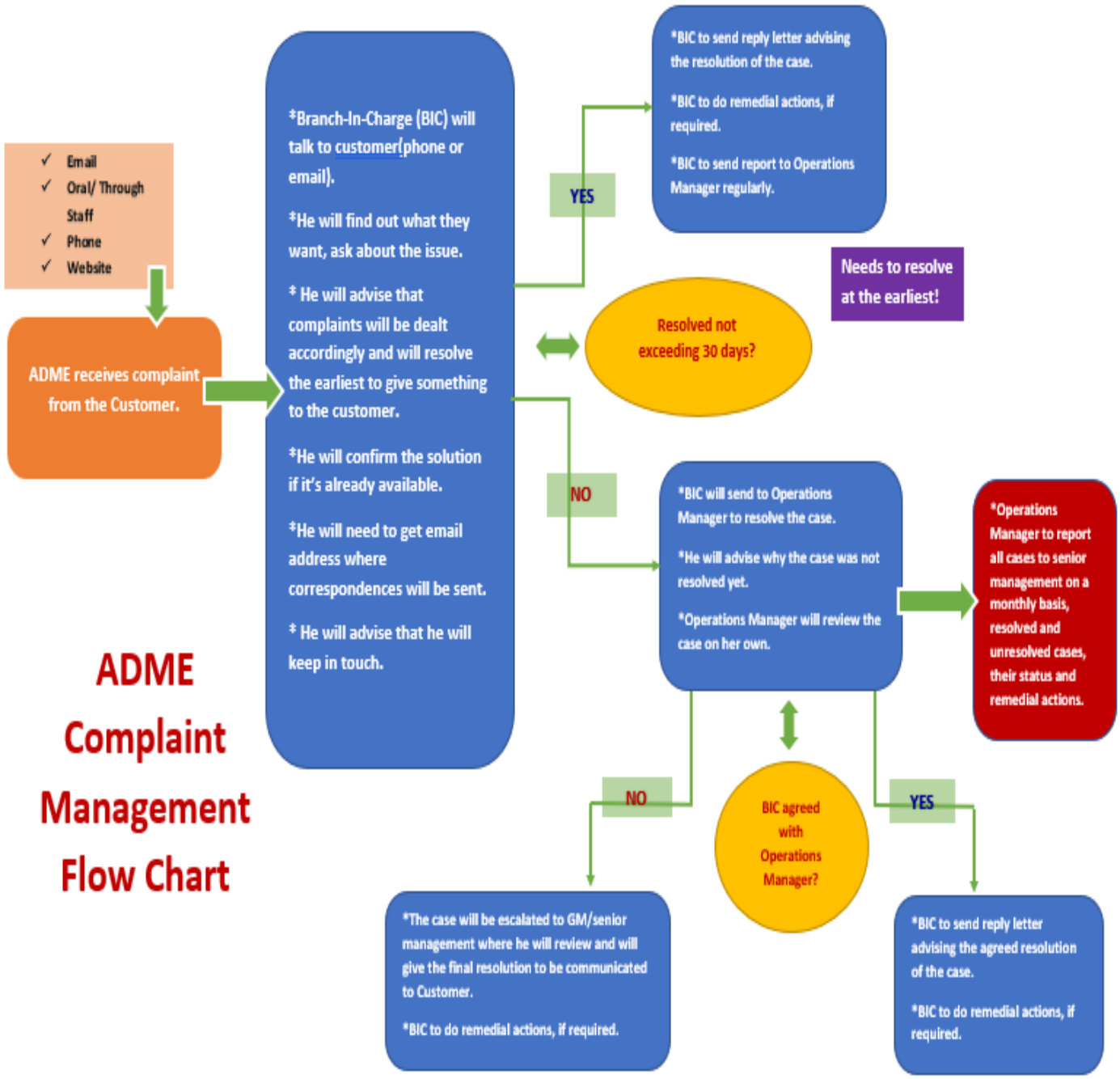
- **ADME ensures that the Central Bank and its Examiners have timely access to any information that may be required to fulfil their responsibilities under the Regulations and the Standards, with respect to outsourced functions.**
- **ADME that our auditors (Internal and External) have timely access to any relevant information that they may be required to fulfil their responsibilities.**
- **ADME ensure that access is given to the Central Bank and the Internal/External Auditors to conduct on-site reviews of outsourced functions at the Service Provider's premises, whenever necessary.**

Complaint Management values -ADME

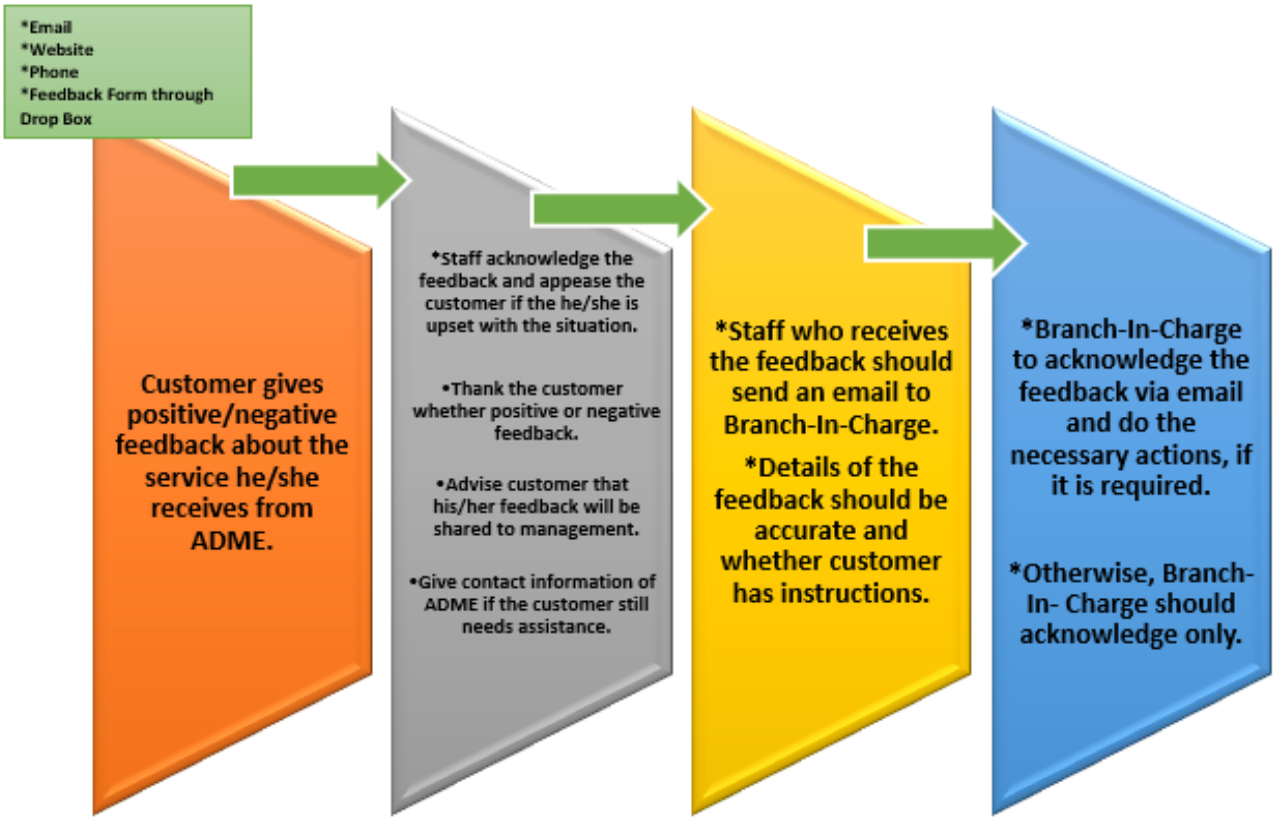
- **ADME establish an independent complaint management function in the organization that directly reports to the Senior Management. The function is empowered to effectively resolve complaints and independent of other business operations.**
- **Enable consumers to make complaints easily and free of cost.**
- **ADME responsibility that consumers are aware of their rights and responsibilities when seeking to resolve their problems or complaints.**
- **Time frames of handling complains must be met.**
- **ADME team Utilize the Data collected to conduct analysis and assess key risks and trends arising out of the Data for conducting investigations into thematic trends, root cause analysis of repeat issues and for designing new controls to address issues and improving quality and efficiency of various aspects of Consumer service**

- **Senior Management will be keep apprised with all issues.**

ADME Complaint Management Flow Chart



ADME Receives "FEEDBACK"



Response Timeframes in Complaints Handling

- **Acknowledgement of your complaint within 2 working days of receipt.**
- **Complaint will be addressed within 15- 30 working days. A relevant response will be sent immediately.**
- **On rare occasions where more time is required for the proper and detailed investigation of your complaint, an extension period will be requested in writing. Inour letter, besides any additional information that we may request, we will inform customer of our actions taken so far and any further actions required for the completion of the investigation.**
- **Our aim is to ensure that you receive our final response within 10 working days from the time of the extension notification or the receipt of any extra information requested from customer.**

ADME Culture of Compliance: ADME establish strong culture of compliance by adopting the following techniques:

- **Train the Staff**
- **Don't make promises you can't keep**
- **Address complaints**
- **Answer your phone**
- **Listen carefully**

Customer feedback and complaints:

Phone: +971-4-2213211

Email: info@aldhaheryexchange.com

Website: www.aldhaheryexchange.com

Suggestion Drop Box at the branch.

Ministry of Economy UAE: The hotline (600-522-225) to receive complaints related to infringements of the rights of the consumers

Record Keeping

ADME maintains an efficient records management program. Which is necessary for proactively and progressively manage all data, media and information. The success of a records management program hinges on the ability to access information for business support, litigation response or compliance reasons. Hence, the records archive has the tools for easy searching, discovery organization and retention management. Record retention is practiced consistently throughout ADME and it works effectively in conjunction with the company's Business Continuity Plan and Disaster Recovery Program. It helps to maintain complete and updated records which is essential for an organization to adequately monitor its relationship with the customer, to understand the customer's ongoing business and activities, and, if necessary, to provide an audit trail in the event of disputes, legal action or investigations that could lead to regulatory actions or criminal prosecution. Further, it helps for accurate and relevant records can other competent authorities, law enforcement agencies of financial intelligence units make effective use of that information in order to fulfil their own responsibilities in the context of AML/CFT. The efficient record keeping enables ADME to demonstrate to the CBUAE, upon request, the adequacy of its assessment, management and mitigation of ML/FT risks; its customer identification and verification policies and procedures; its ongoing monitoring and suspicious transaction reporting process; and all measures taken in the context of AML/CFT.

To Ensure that ADME will be able to provide the identification, verification and KYC information about the customer when required and to reconstruct the transactions undertaken at the request of the relevant authorities at any given time.

- **ADME shall establish a sound and legally compliant record retention policy. Failure to document the necessary KYC and CDD information and keep the prescribed records is an offence.**
- **ADME may have separate policies and procedures for record keeping, active file management, inactive file management, vital records, e-mail management and any other area of records management.**
- **Documents related to transactions, such as outward and inward remittances and foreign currency exchange, must be kept for a minimum period of 5 years from the date of the transaction**

- **Documents and information related to customer profiles, CID, CDD and EDD must be kept for a minimum period of from the date of the transaction**
- **Supporting documents for the transaction monitoring and investigations performed on unusual or suspicious transactions must be kept for a minimum period of 5 years.**
- **Documents related to STRs, including internal disclosures by employees, must be kept for a minimum period of 5 years after the STR was reported. However, in case the matter is under litigation in court or under investigation by an enforcement agency, the supporting documents related to such transactions or STRs must be kept until the court reaches a final verdict or until ADME is notified that the investigation has been closed.**
- **AML training registers, plans and any materials related to the provision of training must be kept for a minimum period of 5 years from the training delivery date.**
- **Records demonstrating compliance with AML/CFT laws and the Standards must be kept for a minimum period of 5 years.**
- **Correspondence related to regulatory enquiries on transactions must be retained for at least 5 years following the termination of the business relationship in order to provide details on such requests to regulators and law enforcement authorities.**
- **Records include electronic communication and documentation as well as physical, hard copy communication and documentation.**
- **Retention may be by way of original documents (i.e., hard copies), stored on microfilm or in electronic form (i.e., soft copies).**
- **Records must be sufficient to permit the reconstruction of individual transactions and provide details of the parties at the request of the relevant authorities.**
- **Records must be made available to the relevant authorities as and when requested**

Records Destruction Policy

Records must be deleted / destroyed when they have reached the conclusion of the retention period.

Retention schedule

Records should be disposed of in a manner which preserves the confidentiality of the record(s). Records that have no retention requirement, and/or duplicate records, must be deleted / destroyed, unless approval to preserve said record is obtained from through the policy coordinator. Records will not be destructed if there are some ongoing regulatory authority/LEA/Correspondents' investigations in progress.

Counterfeit Currency Detection and Reporting

Counterfeit money is an imitation currency produced without any legal sanction of the Government. Producing, circulating or using counterfeit money is a form of fraud/forgery and is a criminal offence. ADME shall implement the Standards guidelines to detect counterfeit currencies and report such incidents to the competent authorities. This policy applies to all employees who are directly or indirectly handling currencies at ADME.

Procedures for Handling Counterfeit Currencies

- **ADME each premises must have counterfeit detection machines and ultraviolet lamps (i.e., UV lamps)**
- **Counterfeit identification training will be given to FLA's.**

- **Internal and external reporting procedures for counterfeit incidents will be given to FLA's.**
- **Appropriate register will be maintained to record counterfeit incident**

Counterfeit Currency Reporting

- **We ensure that such incidents are reported to the police authorities of the respective emirate wherein such incident has occurred.**
- **Report counterfeit currency cases to the FIU as a fraud case via the STR reporting system**
- **Report to the Banking's**
- **Banking Supervision Department of all local currency counterfeit incidents, irrespective of the value of counterfeits using the "Counterfeit Incident Reporting (CIR) Form" (Refer CIR Form)**
- **Report to the Banking Supervision Department of all foreign currency counterfeit incidents, where the total value of counterfeits in a single transaction or multiple transactions by the same person is equal to or above AED 35,000 using the "Counterfeit Incident Reporting (CIR) Form"**
- **Maintain a log register to record full details of every counterfeit incident.**
- **By reviewing such register at the end of every financial year to identify the training requirements for our employees for the following year.**
- **Enabling our staff to submit report internally through ISTR form**
- **Compliance Officer can be notified of the Counterfeit Currency at compliance@aldhaheryexchange.com**

Designated Non-Financial Businesses and Professions (DNFBPs)

A. EDD is required before entering into any business relationship with, or processing any transactions for, DNFBPs as defined under the AML-CFT Decision. DNFBPs may be natural or legal persons.

B. The Licensed Person must implement appropriate, procedures, systems and tools to determine whether a customer is a DNFBP.

C. Where a customer is determined to be a DNFBP, the Licensed Person must carry out the following required steps, in addition to the CDD and EDD required by Paragraph 16.11 of these Standards and any other EDD appropriate to manage the risk of the customer:

- **Verify that the customer is supervised as a DNFBP by the appropriate supervisor;**
- **Obtaining information sufficient to determine that the customer is compliant with the AML/CFT preventive measures required under AML-CFT Decision;**
- **Take additional steps to understand the customer's business and its customer base; and**
- **Obtain approval from the Compliance Officer and the Manager in Charge of the Licensed Person before establishing the business relationship or processing any transactions.**

Dealers in Precious Metals and Stones (DPMS)

A. EDD is required before entering into any business relationship with, or processing any transactions for, DPMS, whether or not they qualify as DNFBPs under AML-CFT Decision. DPMS may be natural or legal persons.

B. The Licensed Person must implement appropriate procedures, systems and tools to determine whether a customer is a DPMS.

C. **Where a customer is determined to be a DPMS, the Licensed Person must carry out the following required steps, in addition to the CDD and EDD required by Paragraph 16.11 of these Standards and any other EDD appropriate to manage the risk of the customer:**
   - **Verifying that the customer has the required licenses;**
   - **Obtaining information sufficient to determine that the customer is compliant with the AML/CFT preventive measures required under AML-CFT Decision;**
   - **Take additional steps to understand the customer's business, including the products and services it offers, its geographic footprint, and its customer base; and**
   - **Obtain approval from the Compliance Officer and the Manager in Charge of the Licensed Person before establishing the business relationship or processing any transactions**

International Bodies

FATF

The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

With more than 200 countries and jurisdictions committed to implementing them. The FATF has developed the FATF Recommendations, or FATF Standards, which ensure a coordinated global response to prevent organized crime, corruption and terrorism. They help authorities go after the money of criminals dealing in illegal drugs, human trafficking and other crimes. The FATF also works to stop funding for weapons of mass destruction.

The FATF reviews money laundering and terrorist financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. The FATF monitors countries to ensure they implement the FATF Standards fully and effectively, and holds countries to account that do not comply

Wolfsberg Group

The Wolfsburg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

The Group came together in 2000, at the Château Wolfsburg in north-eastern Switzerland, in the company of representatives from Transparency International, including Stanley Morris, and Professor Mark Pieth of the University of Basel, to work on drafting anti-money laundering guidelines for Private Banking.

Basel committee

The Basel Committee on Banking Supervision (BCBS) is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions.

USA PATRIOT Act

The USA PATRIOT Act (commonly known as the Patriot Act) was a landmark Act of the United States Congress, signed into law by President George W. Bush. The formal name of the statute is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, and the commonly used short name is a contrived acronym that is embedded in the name set forth in the statute.[2]

The Patriot Act was enacted following the September 11 attacks and the 2001 anthrax attacks with the stated goal of dramatically tightening U.S. national security, particularly as it related to foreign terrorism. In general, the act included three main provisions:

- **expanded surveillance abilities of law enforcement, including by tapping domestic and international phones;**
- **easier interagency communication to allow federal agencies to more effectively use all available resources in counterterrorism efforts; and**
- **increased penalties for terrorism crimes and an expanded list of activities which would qualify for terrorism charges.**

Bank Secrecy Act

- **The Bank Secrecy Act of 1970 (BSA), also known as the Currency and Foreign Transactions Reporting Act, is a U.S. law requiring financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering.[1] Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports if the daily aggregate exceeds $10,000, and report suspicious activity that may signify money laundering, tax evasion, or other criminal activities.[2]**
- **The BSA is sometimes referred to as an anti-money laundering law (AML) or jointly as BSA/AML.[3]**

Penalties

ADME follows regulation of Money Laundering Penalties under UAE Federal Law no (20) of 2018. Articles 14 to 31 of the law describe penalties concerning money laundering offenses, as follows:

Article 14:

The Supervisory authority shall impose the following administrative penalties on the financial institutions, designated nonfinancial businesses and professions and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a) Warning

b) administrative penalties of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) for each violation.

c) Banning the violator from working in the sector related to the violation for the period determined by the supervisory authority.

d) Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.

e) Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.

f) Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority.

g) Cancel the License.

Article 15:

The Financial institutions and designated nonfinancial businesses and professions shall, upon suspicion or if they have reasonable grounds to suspect a transaction or funds representing all or some proceeds, or suspicion of their relationship to the Crime or that they will be used regardless of their value, to inform the Unit without delay, directly and provide the Unit with a detailed report including all the data and information available regarding that transaction and the parties involved, and to provide any additional information required by the Unit, with no right to object under the confidentiality provisions. Lawyers, notaries, other legal professionals and independent legal auditors shall be exempted from this provision if the information related to these operations have been obtained subject to professional confidentiality. The Implementing Regulation of the present Decree-Law shall determine the rules, controls and cases of the obligation to report suspicious transactions

Article 22:

Any person who commits or attempts to commit any of the acts set forth in Clause (1) of Article 2 of this Decree-Law shall be sentenced to imprisonment for a period not exceeding ten years and to a fine of no less than (100,000) AED one hundred thousand and not exceeding (5,000,000) AED five Million or either one of these two penalties. A temporary imprisonment and a fine of no less than AED 300,000 (three hundred thousand dirham) and no more than AED 10,000,000 (ten million dirham) shall be applied if the perpetrator of a money laundering crime commits any of the following acts:

a) If he abuses his influence or the power granted to him by his profession or professional activities.
b) If the crime is committed through a non-profit organization.
c) If the crime is committed through an organized crime group.
d) In case of Recidivism
2 - An attempt to commit a money laundering offense shall be punishable by the full penalty prescribed for it.

3 - A life imprisonment sanction or temporary imprisonment of no less than (10) ten years and penalty of no less than AED 300,000 (three hundred thousand dirham) and no more than AED 10,000,000 (ten million dirham) is applied to anyone who uses Proceeds for terrorist financing.

4 - A temporary imprisonment sanction and a penalty of no less than AED 300,000 (three hundred thousand dirham) shall be applicable to anyone who uses the Proceeds in financing illegal organizations. 5 - The Court may commute or exempt from the sentence imposed on the offenders if they provide the judicial or administrative authorities with information relating to any of the offenses punishable in this article, when this leads to the disclosure, prosecution, or arrest of the perpetrators.

Article 23:

1 - A penalty of no less than AED 500,000 (five hundred thousand) and no more than AED 50,000,000 (fifty million dirham) shall apply to any legal person whose representatives or managers or agents commit for its account or its name any of the crimes mentioned in this Decree-Law.

2 - If the legal person is convicted with terrorism financing crime, the court will order its dissolution and closure of its offices where its activity is performed.

3 - Upon issuance of the indictment, the court shall order the publishing of a summary of the judgment by the appropriate means at the expense of condemned party.

Article 24:

Imprisonment and a fine of no less than AED 100,000 (one hundred thousand) and no more than AED 1,000,000 (one million dirham) or any of those two sanctions is applied to anyone who violates on purpose or by gross negligence the provision Article (15) of this Decree Law.

Article 25:

Imprisonment for no less than six months and a penalty of no less than AED 100,000 (one hundred thousand dirham) and no more than AED 500,000 (five hundred thousand dirham) or any of these two sanctions shall apply to anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated by the Competent Authorities.

Article 28:

Imprisonment or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) shall be applied to any person who violates the instruction issued by the Competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions.

Article 30:

Imprisonment and a fine or one of the two penalties shall be imposed on anyone who intentionally fails to disclose or refrains from providing additional information upon request, from him or deliberately conceals information that must be disclosed or deliberately presents incorrect information, in violation of the provisions provided for in Article 8 of this Decree-Law. Upon conviction, the Court may rule on the confiscation of seized funds without prejudice to the rights of others acting in good faith

Article 31:

Imprisonment or a fine of no less than AED 10,000 (ten thousand dirhams) and no more than AED 100,000 (one hundred thousand dirhams) shall be applied to any person who violates any other provision of this Decree-Law.

Queries and Escalation

CBUAE Queries & Escalations

ADME commits itself to submission of timely and accurate information to the regulatory bodies without delay and on a timely basis. These queries may be solicited on a regular basis or on time to time by the regulatory and other law enforcement bodies in the UAE. ADME ensures that all Circulars and Notices issued by the Central Bank of UAE and Law Enforcement Authorities are implemented, responded to within the time specified by the enforcement body. Where there is no time specified, ADME shall respond to such a notice within 7 working days from the receipt of the notice.

Correspondent Bank Queries & Escalations

Our CBQ process is designed to encourage the fast and efficient resolution of the issues and queries at the first point of contact. We will always aim to provide with satisfactory correspondence information about our on-going payments.
Remittance Operations Officer is empowered to resolve first level queries and make fair and reasonable amendments decisions based on the data collected while conducting EDD. If a Remittance Operations Officer is not able to resolve a query it can be escalated to a Compliance Department on:

Email ID: compliance@aldhaheryexchange.com

During the course of your query about any transaction, we will aim to tailor any proposed resolutions to provide a fair and reasonable outcome to all parties involved. Once accepted, we will aim to deliver our mutually agreed resolution to you within 2 to 3 business days, or 2 business days where the query is urgent.

Urgent Queries

If query is urgent, please reach us as soon as possible via telephone or by email. We will refer case for investigation to Chief Compliance officer on priority basis and will send our response within one business day. We aim to resolve all complaints within 2 business days from the date of initial lodgment. Complex problems will be resolved within 5 business days. We will contact directly to request and discuss a new timeframe in the event that a resolution may fall outside these timeframes. Top priority queries related to our transactions should reach to the higher management at ADME.

Email: info@aldhaheryexchange.com
Phone: +971 4 221321

TF/PF Policy Inclusions:

Targeted Financial Sanctions

The term targeted sanctions means that such sanctions are imposed against specific individuals or groups, or undertakings.

The term targeted financial sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of individuals, entities, groups, or organizations who are sanctioned.

OBLIGATIONS ON UAE PERSONS TO IMPLEMENT TFS REGIMES

- **Guidance for licensed financial institutions on the implementation of targeted financial sanctions dated July 04, 2021**
- **Targeted Financial Sanctions Thematic Review Report, 2023**

Register:

Register at the Executive Office website to receive automated email notifications: https://www.uaeiec.gov.ae

We have registered on the Executive Office's website in order to receive automated email notifications with updated and timely information about the listing and de- listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List. These are done by The Financial Institution regularly and confirmations are submitted.

Screen:

When a match is found through the screening we will immediately, without delay and without prior notice, freeze all funds. "Without delay" means within 24 hours of the listing decision being issued by the UN Security Council or the UAE Cabinet, as the case may be.
Sanction screening is applied in the below cases as follows

a) **In the case of all transactions, the customer's name must be screened against the sanction lists.**
b) **Every customer before On-boarding, and on change of any basic parameters and before verifying a transaction is screened against the TFS List.**
c) **Where the transactions are conducted by a legal person or legal arrangement, the name of the authorized person who carries out the transaction (i.e., the representative) are screened against sanctions lists in addition to the name of the legal person or legal arrangement and its UBOs.**

Apply:

In line with the regulatory requirements on Target Financial Sanctions, The Financial Institution shall ensure the fulfilment of the below mentioned regulatory obligations:

Senior Management should have close oversight over Regulated Entities' Sanctions Risk Framework, TF/PF Risk Assessment outcomes, policies, and processes, including oversight on published Notices and Guidelines by Supervisory Authorities.

- **The owner/ Senior Management shall be regularly updated on the implementation of its Sanction Compliance Programs, including the output and performance of its sanctions screening tools. Reporting metrics shall include trends, and reports generated by sanction screening systems and/or by sanction screening alert review and investigation teams.**

- **The owner/ Senior Management shall establish a strong Compliance culture, setting a clear tone-from-the-top to effectively implement TF/PF controls. The Owner/ senior management shall build the necessary infrastructure supported with adequate skilled resources, tools and systems to appropriately implement TFS requirements.**
- **The owner/Senior Management shall establish clear lines of accountability and responsibilities for TFS compliance.**
- **The Owner/ Senior Management shall ensure it establishes dedicated teams to test the effectiveness of TF/PF controls through Quality Assurance/Audit function.**

Business Risk Assessment

The Financial Institution shall identify, evaluate, and understand the ML, TF, and PF risks in a manner commensurate with the nature and size of the business. This assessment shall be documented and continually updated. The Financial Institution shall be aware of regulatory or law enforcement advisories, and/or global terrorism financing ("TF") and the financing of proliferation of weapons of mass of mass destruction ("PF") trends and risks and consider them as part of their risk assessment process.

The Financial Institution shall:

- **Undertake and document an assessment of the likelihood of dealing with an individual or entity on a Sanctions list. This assessment shall be derived from the UAE's National Risk Assessment, Topical Risk Assessments, guidance and typologies circulated by the Supervisory Authorities and the EOCN.**
- **As part of the risk assessment process, the Financial Institution shall develop and maintain a comprehensive written sanctions risk appetite approved by the owner/senior management and embedded through policies, procedures, and screening systems parameterization.**
- **Ensure that the risk assessment remains current and up to date based on changes (e.g., new product or services or the use of new delivery channel) to the business, and that comprehensive components pertinent to TF/PF risk mitigation measures in line with the business nature and size are incorporated in the assessment.**

Further, The Financial Institution shall,

- **Ensure to implement freezing measures, without delay, if a customer is listed by the UN Consolidated List and UAE Local Terrorist List. Subsequently, the Supervisory Authority is notified immediately of action taken and provides information on the sanction person and/or entity.**
- **Ensure prohibition of making funds available to the customer.**

- **Register on the EOCN's website to receive notifications related to any new listing, re-listing, updating, or de-listing decisions issued by the UN Security Council, the UAE Supreme Council.**
- **Ensure that the appointed Compliance officer is aware of the TFS registration obligation and has subscribed to the EOCN Notification System. The Financial Institution shall avoid using personal accounts and register through official email addresses that represent The Financial Institution.**

TFS Reporting

The FFRs and PNMRs shall be submitted to report name matches on the UN Consolidated List and UAE Local Terrorist List. If the Financial Institution identifies persons on other sanctions lists (e.g., OFAC, UK HMT, EU) or the persons appears in screening results for non-related TFS crimes (e.g., criminal charges brough in other countries), the same shall be reported using an STR/SAR Forms.

In the case where there is a partial name match, the Financial Institution has internal procedures in place to manage the customer account and relationship post reporting.

Suspicious Transaction Report and Suspicious Activity Report

A Suspicious Transaction Report and Suspicious Activity Report serves as Exchange's policy for monitoring and detecting suspicious activity or transactions in relation to potential money laundering or terrorist financing.

It is all employee responsibility to promptly notify the Compliance Officer/ACO and provide them with all relevant details, where the employee either know, suspect, or have reasonable grounds for knowing or suspecting that a person is engaged in or attempting money laundering or terrorist financing.

Once the employee notifies the CO about his/her suspicion, CO is required to investigate and document the circumstances for the suspicion. Based on the investigation the CO will decide whether to file the SAR. The SAR is to be filed through go AML portal of Financial Intelligence unit of CBUAE. Whether an SAR is filed with the authorities or not, the CO ensures that all documents in relation to the transaction, client and any other materials evidencing the investigation are retained.

Following points to be noted while raising an SAR:

- **Raise SAR with all details and copies of all applicable documents; forward it immediately to the CO.**
- **SAR should be raised even for attempted transactions: Attempted transactions are those where the customer did not complete the transactions. Confidentiality should be maintained with respect to any suspicion.**

When transaction is suspected having links to terrorism financing:

- **Immediately block the transaction (process it in the system but should not be transmitted)**
- **Transaction will remain frozen till feedback and further instructions are received from FIU, of CBUAE.**

Reporting of Suspicious transactions and activity is mandatory:

It is the duty of all staff / officers to report suspicious and unusual transactions to the Compliance Officer (Internal reporting of STR).

In case of a transaction suspected of terrorism or terrorist organization, it should be frozen and should be informed FIU immediately.

When an employee suspects a transaction/ activity to be suspicious, he/she should report his suspicions to their Compliance Officer, who will investigate and if found suspicious, will report the case in STR/SAR to the Central Bank of UAE through go AML portal of FIU.

Identifying and Designating persons or entities financing WMD Proliferation

To comply with and fulfil the preventive intent of the relevant UNSCRs, it is necessary for countries to be able to identify specific information supporting a determination and to propose additional persons and entities, as appropriate, to the UN Security Council or the relevant Committee for designation. Noting the increasingly prevalent use of sophisticated sanctions evasion techniques by proliferation networks (e.g., the use of multiple shell and front companies), it is important that countries submit information on these activities to the UN for potential listing. While there is no specific obligation upon countries to submit designation proposals to the relevant Security Council or its Committee, the UN Security Council, or the Committee, in practice, depends upon requests for designation by countries. The Interpretive Note to Recommendation (7) specifically mentions in its paragraph 4 that countries should consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the UN Security Council for designation in accordance with relevant UNSCRs which impose targeted financial sanctions (TFS) in the context of the financing of proliferation of weapons of mass destruction. The countries should have appropriate legal authorities and procedures and should consider establishing or identifying a competent authority or authorities, to solicit and consider information from all relevant sources to identify, and to collect as much identifier information as possible about persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for "designation". In addition, the financial institutions should note that the screening of names and addresses against the consolidated list of designated persons and entities (including entities owned or controlled by them) published by the UN Security Council or its Committee is necessary in ensuring compliance with certain elements of targeted financial sanctions.

Dual Usage Goods

According to Article 15 of Federal Decree-law No. (20) of 2018 On Anti-Money Laundering And Combating The Financing Of Terrorism And Financing Of Illegal Organizations (amended by Federal

Decree Law No (26) of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018) and Section 5 of Cabinet Decision No. (10) of 2019 Concerning The Implementing Regulation Of Decree Law No. (20) Of 2018 On Anti- Money Laundering And Combating The Financing Of Terrorism And Illegal Organizations (CD 10) set out the legal obligations on FIs, Red Flags on PF Dealings with dual-use (DUG) or controlled goods example: o Chemicals o DUG (wire nickel, inverters, etc.) referring to Cabinet Decision no 50 of 2020 and UNSCR 1718 (2006) to be reported to EOCN office. The EOCN classified these three lists as DUG:

> **Strategic goods are the dual-use goods, technology and software that can be used for both civilian and military applications, and/or contribute to the proliferation of Weapons of Mass Destruction.**
> **Chemicals components which has dual-use applications for both civilian and military, and/or contribute to the proliferation of Weapons of Mass Destruction as enlisted by the Organization for the Prohibition of Chemical Weapons (OPCW).**
> **Armoring Request the Executive Office for Control and Non-Proliferation issues permits related to import/export/re-export/ transit of armored vehicles and related spare parts and armored glass intended to be used for security or humanitarian purpose. Armored vehicles include land, marine and amphibious vehicles.**

Restrictions on export or import of certain categories of shipments are a key element of many proliferation-related sanctions regimes, both multilateral or unilateral, and national trade-related legislation. "Dual-use goods" include materials, equipment and technology used for legitimate civilian purposes that can also be used in (or may be a necessary component of) military and WMD programs.

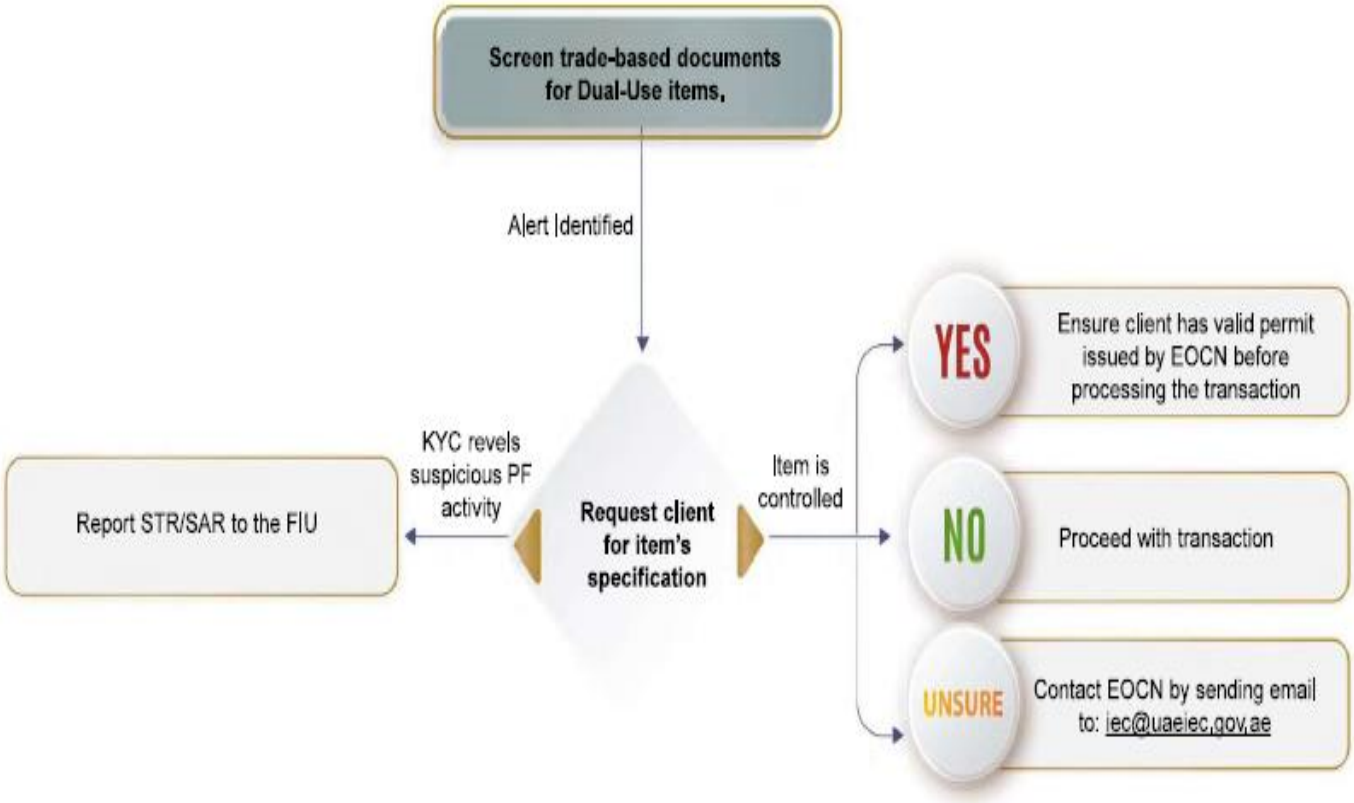
The Financial Institution will:

- **Conduct an Enhanced Due Diligence at the time of onboarding and during transactional stage for the companies which are trading with dual use goods.**
- **Ensure that customers dealing in Dual-Use Items have a valid permit to conduct such trades.**
- **Screen all the goods involved in the trade transaction against the dual use goods list.**

The Executive Office of Control and Non-Proliferation publishes lists of materials, equipment and technology that need to be controlled for export/import. The dual use goods can be accessed from the link given below:

https://www.uaeiec.gov.ae/en-us/control-list-good

The FI will at all times keep the UAE control list downloaded and will check any trade-based document with the list and will take action as depicted below.



Recommendation 7 of the FATF Standards requires countries to implement proliferation financing-related Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions (UNSCRs or resolutions). FATF Recommendation 2 requires countries to put in place effective national cooperation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction (WMD). Immediate Outcome 11 and certain elements of Immediate Outcome 1 relating to national cooperation and coordination aim to measure how effective countries are implementing these Recommendations.

The United Nations Security Council (UNSC or UN Security Council) has a two-tiered approach to counter proliferation financing through resolutions made under Chapter VII of the UN Charter and thereby imposing mandatory obligations for UN Member States.

Red Flags Indicators for Proliferation Financing

To identify a suspicion that could be indicative of proliferation financing activity, FIU has prepared the red flags indicators that are specially intended as an aid for the reporting entities. These red flags may appear suspicious on their own; however, it may be considered that a single red flag would not be a clear indicator of potential proliferation financing activity. A combination of these red flags, in addition to analysis of expected overall financial activity, business profile may indicate towards potential proliferation financing activity.

- **Transaction involves a person or entity in foreign country of proliferation concern.**
- **Transaction involves a person or entity in a foreign country of diversion concern.**
- **The customer or counterparty or its address is like one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.**
- **Customer activity does not match business profile, or end-user information does not match end user's business profile.**
- **A freight-forwarding firm is listed as the product's destination.**
- **Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.**
- **Transaction involves shell companies (e.g., companies do not have a high level of capitalization or display other shell company indicators).**
- **Transaction demonstrates links between representatives of companies exchanging goods i.e., same owners or management.**
- **Circuitous route of shipment (if available) and/or circuitous route of financial transaction.**
- **Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.**
- **Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g., does the country involved normally export/import goods involved).**
- **Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.**
- **Based on the documentation obtained in the transaction, the declared value of the shipment was obviously undervalued vis-à-vis the shipping cost.**
- **Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, destination etc.**
- **Customer vague/incomplete on information it provides, resistant to providing additional information when queried.**
- **Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.**
- **Involvement of items controlled under WMD export control regimes or national control regimes.**
- **Involvement of a person connected with a country of proliferation concern (e.g., a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.**
- **Use of cash or precious metals (e.g., gold) in transactions for industrial items.**
- **Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.**
- **Customers or counterparties to transactions are linked (e.g., they share a common physical address, IP address or telephone number, or their activities may be coordinated).**
- **Involvement of a university in a country of proliferation concern.**
- **Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.**
- **Evidence that documents or other representations (e.g., relating to shipping, customs, or payment) are fake or fraudulent.**
- **Use of personal account to purchase industrial items.**

The following Red-Flags are specific to proliferation Financing cases related to the UAE and other regional countries:

- **The use of representative offices of UNSC sanctioned banks to remit DPRK labors money to DPRK.**
- **The use of extensive currency exchange networks to transfer bulk cash to Iranian nuclear program.**
- **The use of cyber-attacks by the DPRK regime to steal funds from FIs and crypto currency exchanges.**
- **Transactions involved in sale, shipment, or export of dual use goods on incompatible with technical level of the country being shipped (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry).**
- **Trade finance transactions involved shipment routes with weak export control laws.**
- **Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.**
- **The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.**
- **Dealings with sanctioned goods or under embargo. For example:**
  - **Weapons**
  - **Oil or other commodities**
  - **Luxury goods (for DPRK sanctions)**
- **Dealings with controlled substances / Dual-Use items.**
- **Identifying documents that were forged or counterfeited.**
- **Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.**
- **When the flows of funds exceed those of normal business (revenues or turnover).**

Customer Behavior:

- **When the customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to higher risk jurisdictions.**
- **When a customer or counterparty, or its address, is the same or like that of an individual or entity found on publicly available sanctions lists.**
- **The customer is a research body connected with a higher risk jurisdiction of proliferation concern.**
- **When a customer's activities do not match with the business profile provided to the reporting entity.**
- **When a customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.**
- **When a customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.**
- **When a freight forwarding / customs clearing firm being listed as the product's destination in the trade documents.**

- **When destination of goods to be imported / exported is unclear from the trade related documents provided to the reporting entity.**

Transactional Patterns:

- **Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.**
- **The transaction(s) involve an individual or entity in any country of proliferation concern.**
- **The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.**
- **The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e., where the country involved does not normally export or import or usually consume the types of goods concerned.**
- **Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.**
- **When goods destination/shipment country is different from the country where proceeds are sent/ received without any plausible reason.**

Screening Systems

The Financial Institution shall have effective screening systems appropriate to the nature, size and risk of their business and conduct quality control checks on a regular basis.

The Financial Institution shall screen the client database on an ongoing basis and immediately after lists are updated. Associated parties, such as Directors and Beneficial Owners shall be considered when conducting TFS checks. The Financial Institution is also aware of dual-used goods lists issued by the EOCN.

The Financial Institution shall maintain a clear audit trail for any potential matches and are required to document the underlying TF/PF risks.

Training

The Financial Institution shall have tailored TFS training programs and ensures mandatory attendance by all employees.

Trainings cover sanction-related requirements, TFS internal controls, and TF/PF threats, risks, vulnerabilities, and sanction evasion typologies.

All new employees and Senior Management shall undergo necessary TFS training.

The Compliance Officer, alternate Compliance Officer and employees within Sanctions units/departments, if applicable) shall attend TFS training sessions held by the EOCN.

Financing of Illegal Organizations

Like the financing of terrorism, the AML-CFT Law designates the financing of illegal organizations as a criminal offence that is not subject to the statute of limitations. The Law defines the financing of illegal organizations as:

Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by an illegal organization or by any person belonging to an illegal organization or intended to finance such illegal organization or any person belonging to it, even if without the intention to conceal or disguise their illicit origin.

Providing, collecting, preparing, obtaining proceeds or facilitating their obtainment by others with intent to use such proceeds, or while knowing that such proceeds will be used in whole or in part for the benefit of an Illegal organization or of any of its members, with knowledge of its true identity or purpose.

When assessing their risk exposure to the financing of illegal organizations, ADME pay special attention to the regulatory disclosure, accounting, financial reporting and audit requirements of organizations with which they conduct Business Relationships or transactions.

This is particularly important where non-profit, community/social, or religious/cultural organizations are involved, especially when those organizations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason.

Occasional Transactions

During the course of business, EH may be called upon to perform occasional or non-recurring transactions for customers with whom there is no ongoing account or Business Relationship. Examples of such transactions include, but are not limited to:
Exchange of currencies;
Issue or cashing/redemption of traveler's cheques;
Transfer of money or other value for a walk-in customer;

On such occasions LFI is required to identify the customer and verify the customer's identity as well as that of the Beneficial Owners, beneficiaries, and controlling persons. Furthermore, LFI required to undertake appropriate risk-based CDD measures Customer Due Diligence (CDD) Measures, Enhanced Due Diligence (EDD) Measures, Simplified Due Diligence (SDD) Measures for further guidance, including among other things understanding the nature of the customer's business and the purpose of the transaction, in the cases specified in Article 6 of
the AML-CFT Decision, as follows:

When carrying out occasional transactions in favor of a customer for amounts equal to or exceeding AED 55,000 (or equivalent in any other currency), whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;

When carrying out occasional transactions in the form of Wire Transfers for amounts equal to or exceeding AED 3,500 (or equivalent in any other currency) LFI will follow CDD Requirements Concerning Wire Transfers.

Requirements for Correspondent Relationships
(AML-CFT Decision 25)

Financial Institutions are obliged to fulfil certain due diligence requirements with regard to the correspondent banking relationships and other similar relationships they maintain, regardless of whether these involve foreign or domestic financial institutions. Additional guidance in respect of the measures specified in the relevant article of the AML-CFT Decision is provided below. Similar relationships to which FIs should apply the guidance below include, for example those established for securities transactions or funds transfers.

LFI is prohibited from entering into or maintaining correspondent relationships with shell banks, or with institutions that allow their accounts to be used by shell banks. The AML-CFT Decision defines a shell bank as a "bank that has no physical presence in the country in which it is incorporated and licensed, and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision."

LFI is required to collect sufficient information about any receiving correspondent institution for the purpose of identifying and achieving a full understanding of the nature of its business, and to determine, through publicly available information, its reputation and level of AML/CFT controls, including whether it has been subject to a ML/FT investigation or regulatory action.

LFI is obliged to evaluate the AML/CFT controls applied by the receiving correspondent institution.

LFI is required to obtain approval from senior management before establishing new correspondent relationships.

LFI is obliged to understand the responsibilities of each institution in the field of combating the crimes of money laundering, the financing of terrorism and of illegal organizations. Regulatory and supervisory environments governing the operation of financial institutions around the world vary greatly.
Thus, not all foreign financial institutions are subject to the same AML/CFT requirements as FIs in the UAE;
and as a consequence, some of these foreign institutions may pose a higher ML/FT risk. To mitigate against these risks, LFI that maintain correspondent relationships with foreign financial institutions should consider implementing adequate procedures to assess and periodically review the relevant regulatory and supervisory frameworks of the countries concerned.

Furthermore, when gathering information about financial institutions with which they maintain correspondent relationships, whether foreign or domestic, LFI should take appropriate steps to assess the nature, size and extent of their businesses in the countries where they are incorporated and licensed, as well as their ownership and management structures (taking into consideration the nature and extent of any PEP involvement), in order to evaluate whether they exhibit the characteristics of shell banks, and whether they offer downstream correspondent services (also known as "nested accounts") to other banks. If they do offer downstream correspondent services, LFI should also take reasonable steps to understand the types of services offered, the number and types of financial institutions they are offered to, the types of customers those institutions serve, and to identify the associated ML/FT risk issues. In order to collect sufficient information about the nature of a financial institution and the AML/CFT controls it applies, and to assess the ML/FT risks associated with it, LFI should take appropriate measures such as implementing a suitable correspondent relationships questionnaire and, when necessary, conducting follow-up interviews. (LFI may find the correspondent banking questionnaire which has been developed by the Wolfsberg Group, as well as the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking.

In addition to obtaining senior management approval prior to establishing new correspondent relationships, LFI will do periodically review and update their due diligence information in relation to the financial institutions with which they maintain correspondent relationships, commensurate with the risks involved Updating the Customer Due Diligence Information. In the event of a deterioration in the risk profile of a financial institution with which a correspondent relationship is maintained, including the discovery of material adverse information concerning the institution, LFI will ensure that senior management is informed and appropriate risk-based measures are taken to assess and mitigate the ML/FT risks involved. LFI will also maintain agreements or contracts with financial institutions with which they maintain correspondent relationships. In addition to operational details concerning the
products and services covered, these agreements should clearly describe each party's responsibilities in regard to ML/FT risk mitigation, due diligence procedures, and the detailed conditions related to any permitted third-party usage of the correspondent account.

Ongoing Monitoring of Business Relationships

(AML-CFT Law Article 16.1(b), (f); AML-CFT Decision Article 24.2-4)

EH is required to retain all customer records and documents obtained through the ongoing monitoring of Business Relationships. Examples of such records include but are not limited to:

- **Transaction review, analysis, and investigation files, with their related correspondence;**
- **Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls) related to those transactions or their analysis and investigation;**
- **CDD records, documents, profiles or information gathered in the course of reviewing, analyzing or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions;**
- **Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence.**

Post STR/SAR Process

Once a suspicious transaction or other suspicious information related to a customer or business relationship has been reported to the FIU, the LFIs and DNFBPs should take the following immediate actions:

LFIs and DNFBPs should follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general. In cases where the institution hasn't received any response/query from the FIU, the institution needs to put in place adequate controls like Enhanced due diligence and on-going monitoring activity in line with their own Risk Appetite;

LFIs and DNFBPs should identify all related/associated accounts or relationships of STR or SAR customers and conduct a review on those accounts/relationships to check whether any suspicious transaction(s) has taken place. If yes, appropriate risk-based Enhanced Due Diligence ("EDD") and ongoing monitoring procedures should be implemented.

The customer or business relationship, including the related/associated accounts and relationship to the STR or SAR customers, should immediately be classified as high-risk and appropriate risk-based EDD and ongoing monitoring procedures should be implemented in order to mitigate the associated ML/TF risks.
Unless specifically instructed by the FIU to do so, LFIs and DNFBPs are under no obligation to carry out transactions they suspect, or have reasonable grounds to suspect, of being related to a crime.

Furthermore, unless specifically instructed by the FIU to maintain the business relationship (for example, so that the competent authorities may monitor the customer's activity), it should be the LFI's responsibility to take appropriate steps in order to decide whether or not to maintain the business relationship based on their risk appetite.

Commensurate with the nature and size of their businesses, LFIs and DNFBPs that decide to maintain the business relationship should:

- **Document the process by which the decision was made to maintain the business relationship, along with the rationale for, and any conditions related to, the decision; and**
- **Implement adequate EDD measures to manage and mitigate the ML/TF risks associated with the business relationship, including but not limited to, ensuring the STR or SAR subject is added into the relevant lists for close monitoring such as internal watchlists/blacklists, changing the customer risk rating, etc.;**
- **Obtain approvals from the relevant compliance and business stakeholders;**
- **Ensure that the customer is not tipped off about any SAR or STR reported by LFIs and DNFBPs.**

Glossary

KYC	**Know your customer**
ADME	**Al DHAHERY Money Exchange**
ALCO	**Alternate Compliance Officer**
CTF	**Counter Terrorist Financing**
CBAUE	**Central Bank of the UAE**
CCO	**Chief Compliance Officer**
DIRC	**Declaration regarding import of cash**

CDD	**Customer Due Diligence**
CID	**Customer Identification**
CO	**Compliance officer**
CIR	**Counterfeit Incident Reporting**
CTF	**Counter Terrorist Financing**
EDD	**Enhanced Due Diligence**
EWRA	**Enterprise-wide Risk Assessment**
EU	**European Union**
FATF	**Financial Action Task Force**
FI	**Financial institution**
FLA	**Front Line Assistance**
FIU	**Financial Intelligence unit**
GCC	**Gulf Cooperation Council**
HR	**Human Resource**
HIO	**Head of international organization**
ID	**Identity**
IT	**Information Technology**
ISTR	**Internal suspicious transaction report**
KYC	**Know your customer**
KYCC	**Know your customers customer**
KYE	**Know your employee**
LFI	**Licensed Financial Institution**
MLRO	**Money laundering reporting officer**
ML/FT	**Money laundering/ Financing of terrorism**
MOA	**Memorandum of association**
MSB	**Money service business**
NRA	**National Risk Assessment**
OFAC	**Office of foreign asset control**
OR	**On boarding risk**
OTC	**Over the counter**
OTP	**On boarding transaction profile**
PEP	**Political exposed person**
POA	**Power of attorney**
POS	**Point of sale**
PR	**Profile risk**
RBA	**Risk Based Approach**
SDN	**Special Designated Nationals**
SWIFT	**Society of World Wide Interbank Financial communication**
TMS	**Transaction Monitoring System**
TR	**Transaction Risk**

TFS - PF	**Target Financial Sanctions- Proliferation Financing**
UAE	**United Arab Emirates**
UBO	**Ultimate Beneficial owner**
UID	**Unique identification number**
UN	**United Nations**
USA	**United states of America**