AL RAFIDAIN JEWELLERY TRADING LLC

Anti-Money Laundering, Combating Financing of Terrorism, Counter Proliferation Financing, And Targeted Financial Sanctions (AML/CFT/CPF and TFS) Policies and Controls

Version 2.0 – 2026

Contents

1. DOCUMENT INFORMATION

Document Title	**Anti-Money Laundering, Combating Financing of Terrorism, Counter Proliferation Financing and Targeted Financial Sanctions (AML/CFT/CPF& TFS) Policy, Procedures and Controls**
Department	**Compliance**
Version Number	**2.0**
Effective Date	**26/03/2026**
Distribution	• **New Employees, Managers, Senior Managements, Compliance Associates, All Employees of the Company; and** • **Correspondent banks / Business Partners (if applicable).**

2. DOCUMENT APPROVAL STATUS

The AML / CFT/CPF & TFS Policy Prepared by	Name: Vinod Singh Shekhawat **Compliance Officer**	Signature:
The AML / CFT/CPF & TFS Policy Reviewed & Approved by	Name: Hayder Abdulridha Hasan Alobaidi **Owner**	Signature:

Company Stamp

3. DOCUMENT REVISION HISTORY

Date	Version	Author	Description of amendments
			First issuance of the Policy.
March/2026	2.0	Compliance Officer	Policy is updated with detailed procedures.

4. STANDARDS, GUIDELINES, NOTICES & APPLICABLE LAWS

This policy and procedures are created based on the following resources;

4.1 LAWS AND REGULATIONS

S. No.	Details
1	Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing (replacing Federal Decree-Law No. 20 of 2018 and its amendments)
2	Cabinet Resolution No. 134 of 2025 concerning the Executive Regulations of Federal Decree-Law No. 10 of 2025
3	Cabinet Resolution No. 71 of 2024 concerning the unified list of AML/CFT/CPF violations and administrative fines (replacing Cabinet Resolutions No. 16 of 2021 and No. 53 of 2021)
4	Cabinet Decision No. 74 of 2020 on Targeted Financial Sanctions (TFS) relating to UN Security Council sanctions lists
5	Federal Decree-Law No. 43 of 2021 on Commodities Subject to Non-Proliferation (replacing Federal Law No. 13 of 2007)

4.2 GUIDELINES

S.No.	MOE Guidelines
1	Guidelines for Designated Non-Financial Businesses and Professions
2	Supplemental Guidance for Dealers in Precious Metals and Stones
3	Proliferation Finance Institutional Risk Assessment Guidance
4	Implementation Guide for DNFBPs on CUSTOMER RISK-ASSESSMENT (CRA)
5	Implementation Guide for DNFBPs on CUSTOMER DUE DILIGENCE (CDD)

4.3 CIRCULARS

S.No.	CIRCULARS
1	Circular No. (1) of 2026 (11-03-2026) on Updating the Lists of High-Risk Countries, Countries Subject to Increased Monitoring, and Related Measures
2	Circular No. (5) of 2025 (01-07-2025) on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the counter-measures to be applied by Designated Non-Financial Business & Professions (DNFBPs)
3	Circular No. (1) of 2025 (13-03-2025) MOEC/AML/001/2025 on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs).
4	Circular No. (3) of 2025 (19-03-2025) MOEC/AML/003/2025 on emphasize the importance of screening sanctions and terrorist lists.
5	Circular No. (4) of 2025 (09-06-2025) MOEC/AML/004/2025 on emphasize the importance- Understanding the Importance of the UAE 2024 National Risk Assessment
6	Circular No. (2) of 2022 regarding Implementation of Targeted Financial Sanctions (TFS) on UNSCRs 1718 (2006) and 2231 (2015)
7	Circular No. (1) of 2022 (results of the United Arab Emirates Money Laundering & Terrorist Financing Risk Assessment)
8	Circular No. (8) of 2021 (GoAML Reporting Requirements)
9	Circular No. (5) of 2021 - Reference to our Notice No. 1/2020 dated 16/December/2020 regarding Targeted Financial Sanctions (TFS) Reporting

5. INTRODUCTION

AL RAFIDAIN JEWELLERY TRADING LLC (the Company) is committed to complying with all applicable laws and regulations of the United Arab Emirates relating to Anti-Money Laundering, Combating the Financing of Terrorism, and Countering Proliferation Financing (AMLCFTCPF). This includes full adherence to Federal Decree-Law No. 10 of 2025, Cabinet Resolution No. 134 of 2025 (its Executive Regulations), Cabinet Resolution No. 71 of 2024 (unified violations and fines list), and all relevant Cabinet Resolutions, Ministerial Decisions, Guidelines, and Circulars issued by the Ministry of Economy (MOE), UAE Financial Intelligence Unit (FIU), Executive Office for Control and Non-Proliferation (EOCN), and National Anti-Money Laundering and Combatting Financing of Terrorism and Proliferation Committee (NAMLCFTC). As a Designated Non-Financial Business or Profession (DNFBP) operating as a Dealer in Precious Metals and Stones (DPMS), the Company recognizes the high inherent risks associated with the trading, purchase, sale, import, and export of precious metals, particularly gold, and implements a risk-based approach (RBA) with enhanced controls for high-risk customers, transactions, and jurisdictions as required under Federal Decree-Law No. 10 of 2025.

This Policy sets out the internal procedures, controls, and responsibilities required to ensure compliance with:

- **Federal Decree-Law No. 10 of 2025 (replacing Federal Decree-Law No. 20 of 2018 and its amendments)**
- **Cabinet Resolution No. 71 of 2024** concerning the unified list of AML/CFT/CPF violations and administrative fines (replacing Cabinet Resolutions No. 16 of 2021 and No. 53 of 2021)
- **Cabinet Decision No. 74 of 2020 on Targeted Financial Sanctions (TFS)** relating to UN Security Council sanctions lists
- All directives and guidance issued by the **Ministry of Economy**, the **UAE Financial Intelligence Unit (FIU)**, and the **National Anti-Money Laundering and Combatting Financing of Terrorism and Proliferation Committee (NAMLCFTC)**.

The Company adopts a risk-based approach (RBA) to assess, manage, and mitigate the risks of ML/TF/CPF that may arise from its business activities, customer base, geographical exposure, supply chain, and product offering. This includes enhanced controls for high-risk customers, transactions, and jurisdictions, as required under the 2025 AML law.

All employees, management staff, owners, and authorized representatives are required to understand and comply with the requirements of this Policy. Failure to comply may result in disciplinary action and shall be considered a breach of UAE law.

6. AL RAFIDAIN JEWELLERY TRADING LLC AND AML/CFT/CPF COMMITMENT

“AL RAFIDAIN JEWELLERY TRADING LLC” hereinafter referred as “the Company.”

<u>Our AML Compliance Commitment:</u>

As a Designated Non-Financial Business or Profession (DNFBP) operating in the UAE, company is fully committed to upholding the highest standards of Anti-Money Laundering (AML) compliance in strict accordance with the regulations set forth by the Ministry of Economy. Recognizing the critical role of AML measures in safeguarding the integrity of the jewelry industry, we have established a rigorous compliance framework to prevent, detect, and mitigate risks associated with money laundering and terrorist financing.

Comprehensive Due Diligence & Customer Onboarding:

Prior to initiating any business relationship, companies conduct enhanced due diligence (EDD) to verify customer identities, assess transaction legitimacy, and evaluate potential risks. This includes:

- **Identity Verification**: Confirming customer identities through reliable, independent sources.
- **Risk Assessment**: Evaluating the nature of transactions and customer profiles to identify high-risk activities.
- **Ongoing Monitoring**: Continuously reviewing client transactions to detect and report any suspicious behaviour.

Proactive Transaction Monitoring & Reporting:

We employ advanced monitoring systems to scrutinize transactions in real time, ensuring prompt identification of anomalies or red flags. Should any activity raise concerns, company adheres to regulatory requirements by:

- **Immediately escalating** suspicious transactions to the **Financial Intelligence Unit (FIU)**.
- **Maintaining detailed records** of all reports and actions taken.
- **Conducting internal investigations** where necessary to ensure compliance.

Robust Internal Controls & Employee Training:

To reinforce our AML commitment, company has implemented:

- **Strict Internal Policies**: Clear guidelines for identifying, reporting, and managing AML risks.
- **Regular Staff Training**: Mandatory AML awareness programs to ensure all employees understand their compliance obligations.
- **Periodic Audits**: Independent reviews to assess the effectiveness of our AML controls and procedures.

Collaboration with Regulatory Authorities:

Company maintains an open and cooperative relationship with UAE regulatory bodies, ensuring full compliance during inspections and audits. We actively engage with authorities to align our practices with evolving AML regulations, demonstrating our dedication to transparency, accountability, and ethical business conduct.

By integrating these measures into our operations, company not only protects its business from financial crime but also contributes to the broader effort of maintaining the UAE's reputation as a secure and compliant financial hub.

7. STAGES OF THE SUPPLY CHAIN AND ROLES OF DPMS

The trade in PMS consists of a complex ecosystem or supply chain from extraction of the raw mineral to eventual sale to the final customer, in which numerous participants are involved. DPMS may perform a wide variety of roles or functions relating to the trade in PMS, and in order to understand these roles and the potential ML/FT risks they entail, it is necessary to have a basic understanding of the stages of the supply chain. It should be understood that the supply chains for different PMS may have certain characteristics which are unique to that particular PMS or category of PMS. Furthermore, the supply chain is not necessarily a strictly vertical one, in that different participants may trade with each other in multiple directions at different stages of the chain, and certain stages may run concurrently or be skipped altogether. However, for the sake of convenience, these stages, and some of the major ML/FT risks to which each stage is vulnerable, may be simplified as follows:

Extraction/production: This stage may also include the sorting and grading of raw minerals, and their preparation for sale. Key ML/FT risks at this stage include but are not limited to the infiltration of the extraction/production process by criminal or terrorist organizations; vulnerability of the supply chain to the introduction of illicit PMS, or “commingling”; over-, under-, or false-invoicing and accounting fraud. This stage is also vulnerable to numerous predicate offences, such as theft, embezzlement, smuggling, and bribery/corruption.

Trading in raw minerals: This stage of the supply chain may also involve the export and import of raw ore or rough gemstones. Moreover, the market for different types of raw PMS may have different characteristics and regulatory regimes.

Beneficiation: In this stage of the PMS supply chain, raw minerals are transferred to technically specialized intermediaries for purification and preparation for sale by various processes, such as refining/smelting in regard to precious metal ores and cutting and polishing with respect to precious stones. This stage can also include the recycling of existing PMS (e.g., the re-smelting of scrap precious metals, or the re-cutting and polishing of precious stones). DPMS may participate in this stage of the supply chain as technical specialists (refiners, cutters, polishers, etc.), or as wholesalers, agents, buyers or sellers trading with, or on behalf of, such specialists.

Wholesale trade: In this stage, processed PMS (either refined precious metals or cut and polished precious stones), as well as finished goods (i.e. Jewellery) are traded on a wholesale basis for a variety of purposes, and through diverse channels, some of which may entail the physical exchange of goods and others of which may be virtual in nature (for example, through certificates or various derivative products). Key ML/FT risks at this stage include but are not limited to commingling, trade-based ML, and other known typologies and methods associated with placement, layering and integration.

Retail trade: In this stage, beneficiated PMS or finished goods (in particular Jewellery fabricated from PMS) are sold to, or acquired from, retail customers in the primary or secondary markets. DPMS involved in this stage are usually retail merchants involved in selling or buying direct to/from the public. This stage is particularly vulnerable to ML/FT risks connected with commingling, as well as to the classic ML/FT risks associated with placement, layering and integration, and to predicate offences such as fraud, theft and robbery or embezzlement, among others.

There are many different stages and transactions and counterparties involved in the precious stones and precious metals businesses. As set forth above, miners range from international companies to individuals. Intermediaries may be well established local buyers from miners, or itinerant foreign buyers, or hawalas. Retail jewellers may buy articles of used jewellery, as may direct buyers and pawnshops. Each of these businesses may present a money laundering risk.

Dealers may buy from or sell to other counterparties who also work in their precious metals or precious stones businesses or sell to the public through retail sales (which may often be anonymous). Dealers will need to consider the risks associated with each stage at which they participate. A risk-based approach should account for higher risk customers and counterparties at every stage.
In some sectors within precious metals and precious stones businesses, trust based on personal contact is an essential element of conducting business, and such trust and personal contact assist in lowering counterparty risk. In addition, each industry has trade resources, such as trade associations and directories, with which to establish some background and credit information and these should be consulted. Checks must be made upon any new counterparty that is unknown to a dealer, and particularly if also unknown within the dealer's industry. A counterparty, who proposes a transaction in diamonds, jewels or precious metals should have the knowledge, experience and capacity, financial and technical, to engage in that transaction.

Company has implemented the Anti Money Laundering and Combating Financing of Terrorism and Targeted Financial Sanctions (AML-CFT & TFS) Policies, Procedures, and Controls, version (Version Number). This initiative aims to uphold a strong compliance culture within the organization and mitigate the risks associated with Money Laundering and Terrorist Financing in accordance with the UAE AML compliance laws.

The global challenge of combating money laundering and the financing of terrorism necessitates strict adherence to internationally recognized standards. As such, the Company has established this policy to demonstrate the commitment of its management and employees in adopting the highest standards of AML, CFT, and TFS compliance across all activities and functions.

By implementing these policies, procedures, and controls, the Company aims to proactively prevent and detect any potential instances of money laundering or terrorist financing. These measures serve to safeguard the integrity of the financial system, protect the Company's reputation, and contribute to the overall stability and security of the industry.

The Company recognizes the importance of continuous improvement and will regularly review and update its AML-CFT & TFS framework to align with emerging industry's best practices and regulatory requirements. All employees are expected to fully comply with these policies and actively contribute to maintaining a robust AML, CFT, and TFS compliance program.

8. PURPOSE OF THE POLICY

The purpose of the policy is to effectively implement the key principles of AML/CFT laws and regulations, in line with Ministry of Economy / Committee for Commodities Subject to Import & Export Control / Financial Intelligence Unit, by educating our employees to act as the first line of defense in combating money laundering activities.
The Company accepts only those customers whose source of funds can be reasonably established as legitimate and who do not pose any risk (actual or potential) to the company's reputation. and;

a) Engage only in legitimate business abiding by all relevant rules and regulations which apply to our activities.
b) Maintain the highest ethical and moral standards.
c) Operate always under best practice, exercising due care and all necessary due diligence.
d) Aim to establish long-term relationships with our immediate clients.

9. APPLICABILITY

This policy applies to all staff members, including Senior Management and the Board of Directors (BOD), as well as to all branches, subsidiaries, and any representatives acting on behalf of the Company. Compliance with this policy is mandatory and forms an integral part of each employee's responsibilities.

All staff members are required to comply with Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing, relevant regulations, and internal procedures. This includes adherence to all AML/CFT/CPF obligations.

10. REVIEW & APPROVAL

The AML/CFT Policy and Procedures shall be reviewed and updated, annually at a minimum, to make it consistent with all applicable Laws, Regulations, Notices, Standards and other international best practices and to make it effective in mitigating the existing as well as emerging ML/FT risks.
The review would be done by the compliance officer and approved by the Senior Management.
The policies would be reviewed annually as well as in the event of the following:

- Change in regulatory guidelines of Ministry of Economy / Committee for Commodities Subject to Import & Export Control / Financial Intelligence Unit of the UAE as well as any other relevant authorities.
- Change in business profile/ product mix due to change in business model or market conditions.

11. OVERVIEW OF THE AML/CFT LEGAL, REGULATORY, AND NATIONAL STRATEGY FRAMEWORKS OF THE UNITED ARAB EMIRATES

11.1. NATIONAL LEGISLATIVE AND REGULATORY FRAMEWORK

The legal and regulatory structure of the UAE is comprised of a matrix of federal civil, commercial, and criminal laws and regulations, together with the various regulatory and supervisory authorities responsible for their implementation and enforcement, as well as various local civil and commercial legislative and regulatory frameworks in the Financial and Commercial Free Zones. Criminal legislation is under federal jurisdiction throughout the State, including the Financial and Commercial Free Zones. The crimes of money laundering, the financing of terrorism, and the financing of illegal organizations are covered under federal criminal statutes and the federal penal code. Likewise, federal legislation and implementing regulations on the combating of these crimes are in force throughout the UAE, including the Financial and Commercial Free Zones. Their implementation and enforcement are the responsibility of the relevant regulatory and supervisory authorities in either the federal or local jurisdictions.

The principal AML/CFT/CPF legislation within the State is Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing (the AML/CFT/PF Law or the Law), together with its future implementing regulations, which will supersede prior implementing regulations issued under Federal Decree-Law No. 20 of 2018. Compliance with the AML/CFT/CPF obligations under this Law is mandatory for all persons and entities operating in the UAE, including DNFBPs, financial institutions, and legal entities incorporated in the mainland or Free Zones.

The UAE has issued Cabinet Resolution No. 109 of 2023 on the Regulation of the Procedures of the Real Beneficiary (UBO Resolution). DNFBPs licensed and operating from Financial Free Zones should refer to the regulations governing beneficial ownership and control issued by their relevant Financial Free Zone authority.

The UBO Resolution introduces the requirement for a beneficial ownership register in the mainland UAE and unifies the minimum disclosure requirements for corporate entities incorporated in the UAE mainland and in the non-financial free zones. Compliance with these beneficial ownership requirements is mandatory under Federal Decree-Law No. 10 of 2025 and forms an integral part of the Company's AML/CFT/CPF obligations.

11.2. <u>THE MINISTRY OF ECONOMY</u>

The Ministry of Economy, as the supervisory authority, is entrusted with the supervision of the 'Designated Non-financial Businesses and Professions' (DNFBPs) sector at the state level and commercial free zones in order to combat money laundering and financing of terrorism, **including ensuring compliance with Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing**. It is committed to developing a strong regulatory framework and providing a safe environment for organizations, companies, and DNFBPs to work according to international best practices. It also contributes towards raising the competitiveness of the state's economic, investment and financial environment, building an attractive business and investment climate within various sectors, and creating a balanced, flexible and sustainable future economic model. The priorities include providing all possible forms of knowledge, guidance and training support for Designated Non-financial Businesses and Professions and raising their level of awareness to be able to fulfil their commitments, in partnership with various economic sectors. The main objective of the efforts of the Ministry of Economy at the international level is to raise the level of compliance with international requirements and maintain the top position and positive reputation of the national economy in global markets as well as with all countries and international partner organizations.

11.3. THE EXECUTIVE OFFICE FOR CONTROL AND NON-PROLIFERATION (EOCN)

Executive Office for Control and Non-Proliferation (EOCN) play an active role in implementing export control besides curbing the proliferation of weapons of mass destruction with relevant associated technology, based on policies, legislation and partnerships domestically and internationally. The EOCN was established in the United Arab Emirates in 2009 as a body responsible for implementing the provisions of Federal Decree Law No. (43) of 2021 On the Commodities Subject to Non-Proliferation which replaces Federal Law No. (13) of 2007 Concerning Commodities Subject to Control of Import and Export. This is for the aim of preventing the illegal and unauthorized circulation of dual-use goods that contribute to the production or development of weapons of mass destruction, along with their associated technology and means of delivery.

The Executive Office for Control and Non-Proliferation, in cooperation with the Ministry of Foreign Affairs and International Cooperation (MoFAIC) and other government agencies, exerts extreme efforts in following up the application of the resolutions and requirements of the United Nations Security Council and other relevant international and regional organizations. EOCN also coordinates and supervises the application of targeted financial sanctions and related measures in accordance with Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing, as well as the implementation of Security Council resolutions on the prevention and suppression of terrorism, its financing, and the cessation of arms proliferation, in addition to other relevant resolutions in coordination with competent stakeholders.

The Executive Office is the technical focal point for following up on the UAE's obligations in the Convention on the Prohibition of the Development, Production, Storage and Use of Chemical Weapons. This reflects the UAE Government's vision of maintaining security and stability inside and outside the country and promoting partnership with countries of the region and the rest of the world to be free of weapons of mass destruction.

11.4. AML/CFT NATIONAL STRATEGY FRAMEWORK

Money laundering and the financing of terrorism are crimes that threaten the security, stability and integrity of the global economic and financial system, and of society as a whole. The estimated volume of the proceeds of crime, including the financing of terrorism, that are laundered each year is between 2-5% of global GDP. Yet, by some estimates, the volume of criminal proceeds that are actually seized is in the range of only 2% of the total, while roughly only half of that amount eventually ends up being confiscated by competent judicial authorities. Combating money laundering, the financing of terrorism, and proliferation financing is therefore an urgent priority in the global fight against organized crime.

The UAE is deeply committed to combating money laundering, the financing of terrorism, and proliferation financing. To this end, the Competent Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection and deterrence of financial crimes, including ML/FT/PF. They also continue to work towards reinforcing the capabilities of the resources committed to these efforts, and towards improving their effectiveness by implementing the internationally accepted AML/CFT standards recommended and promoted by FATF, MENAFATF and the other FSRBs, as well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

As part of these efforts, the Competent Authorities of the UAE have taken a number of substantive actions, including among others:

- Enhancing the federal legislative and regulatory framework, embodied by the introduction of Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing, which incorporates the FATF standards.
- Conducting the National Risk Assessment (NRA) to identify and assess the ML/FT/PF threats and inherent vulnerabilities to which the country is exposed, as well as to assess its capacity in regard to combating ML/FT/PF at the national level.
- Formulating a National AML/CFT Strategy and Action Plan that incorporates the results of the NRA, and which are designed to ensure the effective implementation, supervision, and continuous improvement of a national framework for combating ML/FT/PF, as well as providing the necessary strategic and tactical direction to the country's public and private sector institutions in this regard.

The National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism of the United Arab Emirates is based on four pillars, each of which is associated with its own strategic priorities. These strategic priorities in turn inform and shape the key initiatives of the country's National Action Plan on AML/CFT.

The pillars of the National Strategy, together with their strategic priorities, are summarized in the table below:

National AML/CFT Strategic Pillars	Strategic Priorities
Legislative & Regulatory Measures	Increase effectiveness and efficiency of legislative and regulatory policies and ensure compliance.
Transparent Analysis of Intelligence	Leverage the use of financial databases and the development of information analysis systems to enhance the transparent analysis and dissemination of financial intelligence information.
Domestic and International Cooperation & Coordination	Promote the efficiency and effectiveness of domestic and international coordination and cooperation with regard to the availability and exchange of information.
Compliance and Law Enforcement	Ensure the effective investigation and prosecution of ML/FT crimes and the timely implementation of TFS.

The National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations has identified a number of key drivers of success in achieving the goals of the National AML/CFT Strategy. These include, among other things, ensuring:

- Effective coordination between the Financial Intelligence Unit, Law Enforcement Authorities, Public Prosecutors, Supervisory Authorities, and other Competent Authorities within the country;

- Effective compliance with the laws and regulations governing banking activities and other financial services;

- Awareness by DNFBPs of the relevant ML/FT risks facing the UAE in general, and their sectors in particular, as informed by the results of the NRA, as well as their awareness of their statutory obligations in regard to the management and mitigation of those risks.

11.5. UAE ML/TF NATIONAL RISK ASSESSMENT ON THE DNFBP SECTOR

In the UAE, the Designated Non-Financial Businesses and Professions (DNFBP) sector is large and diverse, with around 16,000 firms supervised by four supervisory authorities, the vast majority of which are operating in the mainland and commercial free zones, where 96% of the total DNFBP population are supervised by the Ministry of Economy (MOEc) and 2% by the Ministry of Justice (MOJ). The number of DNFBPs operating in the financial free zone's accounts for around 2% of the total population supervised by the DIFC and the ADGM.

Below are the risk classifications of the DNFBP sector as per the 2024 NRA result:
a) DPMS in the mainland – Medium-High risk
b) DPMS in the Financial Free Zone – Medium Risk
c) Real Estate sector (both mainland and FZ) – High Risk
d) Real Estate sector (FFZ) – Medium-Low
e) Corporate Service Providers (Mainland and FFZ) – Medium Risk
f) The Audit and Accounts Sector (Mainland and Free zones) – Medium-Low
g) Lawyers and Legal Professionals Sector – Medium-Low

Given all the above, it is of critical importance that DPMS are well acquainted with their customer due diligence (CDD) obligations under Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing, as well as with the various risk factors and indicators that can help them to identify and report suspicious transactions related to ML/FT/PF.

12. TARGETED FINANCIAL SANCTIONS (TFS)

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and has primary responsibility for the maintenance of international peace and security. It has 15 Members, and each member has one vote. Under the Charter of the United Nations, all Member States of the UN are obligated to comply with the Security Council decisions.

The UNSC holds the capacity to take action seeking to maintain or restore international peace and security under Article 41 of Chapter VII of the Charter of the United Nations by imposing sanctioning measures. These measures encompass a broad range of enforcement options that do not involve the authorization of the use of armed force, including interruption of economic relations, international communications, and diplomatic relations.

The Security Council sanctions regimes focus mainly on supporting the settlement of political conflicts, nuclear non-proliferation, and counterterrorism. These regimes include measures ranging from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and restrictions on dealing with certain financial or commodity transactions.

In addition, the Financial Action Task Force (FATF), an inter-governmental body responsible for setting international standards on Anti-Money laundering (AML) and countering the financing of terrorism (CFT) and proliferation (CPF), under Recommendations 6 and 7 (R6/R7) of the FATF Standards, requires the implementation of targeted financial sanctions (TFS) to comply with the UN Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism, terrorism financing, and proliferation financing.

The United Arab Emirates (UAE), as a member of the United Nations, is committed to implementing UNSCRs, including those related to the UN's sanctions regimes. Consequently, through the Cabinet Decision No. 74 of 2020, the UAE is implementing relevant UNSCRs on the suppression and combating of terrorism, terrorist financing and countering the financing of proliferation of weapons of mass destruction, in particular relating to TFS. Persons should note that, in accordance with the laws of the UAE, the UAE Government also applies TFS by publishing a Local Terrorist List in accordance with UNSCR 1373 (2001).

12.1. WHAT ARE TFS?

The term TFS refers to **asset freezing** and **prohibition from making funds or other assets or services** available either directly or indirectly, for the benefit of designated individuals, entities, or groups listed in the Sanctions Lists.
Asset freezing without delay: Freezing is the prohibition to transfer, convert, dispose of, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Sanctions Lists, **immediately (within 24 hours)** upon designation. It includes:

- The freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access.
- The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, by selling or mortgaging them.

Prohibition from making funds or other assets or services available: This means the prohibition to provide funds or other assets to or render financial or other services to any designated individual, entity, or groups listed in the sanction list.
Example: FIs: a freezing measure can block access to bank accounts transactions.

DNFBPs: a freezing measure can be stopping the facilitation of or blocking the transfer of ownership of immovable (real estate) or movable assets (gold).
VASPs: a freezing measure can be blocking services to trade and transfer virtual assets, as well as suspending/restricting access to accounts.

12.2.) DURATION OF THESE MEASURES

Asset freezing and prohibition measures have **no time limit**: the funds or other assets remain frozen, and the prohibition from making funds or other assets or services available remains until the individual, entity, or group is removed from the **UAE Local Terrorist Lis**t or the **UNSC Consolidated List** or until there is a freezing cancellation decision communicated by the EOCN

12.3.) PURPOSE OF TFS

The purpose of TFS is to deny certain individuals, entities, or groups the means to violate international peace and security, support terrorism or finance the proliferation of weapons of mass destruction. To achieve this, it seeks to ensure that no funds or other assets or services of any kind are made available to designated persons for so long as they remain subject to the targeted financial sanctions measures.
TFS are implemented in the UAE pursuant to UNSCRs in relation to:

a. <u>Terrorism And Terrorist Financing:</u>

1	Islamic State in Iraq and the Levant (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities.	UNSCR 1267 (1999), 1989 (2011) and its successor resolutions
2	The Taliban, and associated individuals, groups, undertakings, and entities.	UNSCR 1988 (2011) and its successor resolutions
3	Any individual or entity included in the Local Terrorist List, pursuant to UNSCR 1373 (2001)	UNSCR 1373 (2001)
4	Al-Shabaab Sanctions Committee	UNSCR 2713 (2023)

b. The Proliferation of Weapons of Mass Destruction (WMD):

1	Democratic People's Republic of Korea (DPRK): nuclear-related, other weapons of mass destruction-related and ballistic missile-related programs.	UNSCR 1718 (2006) and its successor resolutions

c. Other UN Sanctions Regimes with TFS:

1	Iraq	UNSCR 1518 (2003)
2	Democratic Republic of Congo (DRC)	UNSCR 1533 (2004)
3	Sudan	UNSCR 1591 (2005)
4	Lebanon	UNSCR 1636 (2005)
5	Libya	UNSCR 1970 (2011)
6	Guinea-Bissau	UNSCR 2048 (2012)
7	Central African Republic	UNSCR 2745 (2024)
8	South Sudan	UNSCR 2206 (2015)
9	Haiti	UNSCR 2653 (2022)
10	Yemen	UNSCR 2140 (2014)

12.4.) WHERE TO FIND THE UPDATED SANCTIONS LISTS?

The information on designated individuals, entities, or groups in the Sanctions Lists is subject to change. The most recently updated information can be found in the following links:

- The UAE has a **Local Terrorist List** of all the sanctioned individuals, entities, or groups designated by the UAE Cabinet. The link to the Local Terrorist List can be found at the bottom of the Sanctions Implementation webpage on the Executive Office for Control

& Non-Proliferation's (EOCN) website: https://www.uaeiec.gov.ae/en-us/un-page?p=2#

- The UNSC has a **UNSC Consolidated List** of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC. This link can be found on: https://www.un.org/securitycouncil/content/un-sc-consolidated-list
- The EOCN has created a subscription-based notification system, known as the **EOCN Notification Alert System (NAS),** which automatically sends out any updates to the Sanctions Lists to all subscribed entities

12.5.) WHO IS THE TARGET OF THESE MEASURES?

The freezing measures, including the prohibition of making funds or other assets or services available, apply to:

a) Any individual, entity, or group designated in the Local Terrorist List issued by the Federal Cabinet or designated by the UNSC in the UN Consolidated List.

b) Any entity, directly or indirectly owned or controlled by an individual, entity, or group designated under A.

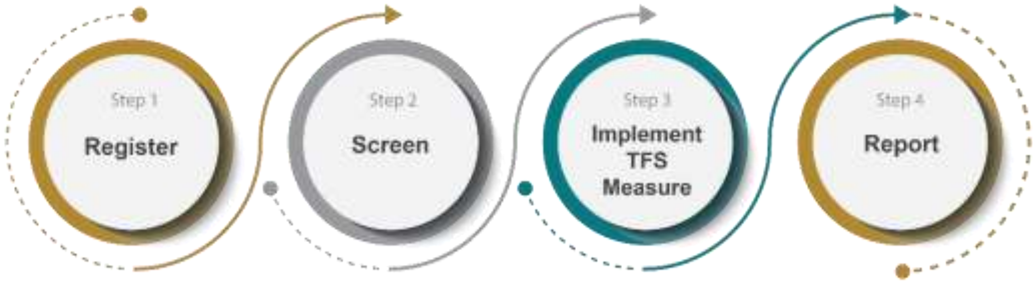
c) Any individual or entity acting on behalf of or at the direction of any individual, entity, or group designated under A & B.

In cases where an asset is owned or controlled in part or in full by a designated individual, entity, or group and such asset continues to produce benefit, for example in the form of dividends or interest, the relevant portion of such benefit is also subject to freezing measures.

12.6.) TARGETED FINANCIAL SANCTIONS AS PER FATF RECOMMENDATIONS

Terrorist Financing (TF)	**Proliferation Financing (PF)**
• ISIS & Al-Qaida UNSCR 1267, 1989 • The Taliban UNSCR 1988 • UAE Local Terrorist List UNSCR 1373	• Democratic People's Republic of Korea (DPRK) UNSCR 1718 (2006) • Islamic Republic of Iran UNSCR 2231 (2015)

12.7.) OBLIGATIONS TO IMPLEMENT TFS



12.8.) Register

- Reporting Entities are required to register to the **Notification Alert System (NAS)** on the EOCN's website to receive automated email notifications on any updates to the Sanctions Lists: https://www.uaeiec.gov.ae/en-us/un-page
- This registration is aimed at helping Reporting Entities receive updated and timely information about the designation, de-listing, or amendments of individuals, entities, or groups designated in the Sanctions Lists.

12.9.) SCREEN

Undertake regular and ongoing screening on the latest sanction list. Screening must be undertaken in the following:

- Upon any updates to the Sanctions List. In such cases, screening must be conducted immediately and without delay to ensure compliance with implementing freezing measures without delay (within 24 hours).
- Prior to onboarding new customers.
- Daily screening of customer's databases
- Upon periodic KYC reviews or if there is a material change in the nature or ownership of the customer.
- Before processing any transaction of a counterparty

The following database is also included in the screening process:

- Existing customer databases. All systems containing customer data and transactions need to be mapped to the screening system to ensure full compliance
- Previous customers with no current active accounts/relationship up to a period of 5 years
- Names of parties to any transactions (e.g., buyer, seller, agent, freight forwarder, etc.)
- Potential customers before conducting any transactions or entering into a business relationship with any person.
- Ultimate Beneficial owners, both natural and legal
- Names of individuals or entities with direct or indirect relationships with them.
- Customers before conducting any transactions or entering a business relationship with any Person.

- Directors and/or agents acting on behalf of customers (including individuals with power of attorney)

The following are examples of the identifiers in the Sanctions Lists:

Screening for Natural Person:

- Individual's Name
- Date of birth
- Nationality
- ID or passport Number
- Last known address

For Legal Persons & Arrangements

- Entity or Company's Name (s)
- Trade License number
- Address of registration
- Address of branches
- Other information (Because many names are very common, you may find various potential matches. However, it does not necessarily mean that the individual or entity you are dealing with is subject to TFS)

Types of Matches (Results)

A. **Partial Name Match/Potential match** –A Partial Name Match is when there is a partial match between the key identifiers in the UAE Local Terrorist List or UNSC Consolidated List and a customer's information in your database, and you are unable to conclude a False Positive or a Confirmed Name Match.

B. **Confirmed Name match**- A confirmed name match is when an individual, entity, or group matches all of the key identifiers published on the UAE local Terrorist List or UNSC consolidated List.

C. **False positive result** - A False Positive is a match to listed individuals, entities, or groups, which upon examination of key identifiers, such as full name, DOB, and nationality, proves not to be the designated individuals, entities, or groups.

D. **Negative Match-** A Negative Match is when no match is identified upon conducting screening.

On **weekends and public holidays**, companies have appropriate internal procedures to effectively screen against the UAE Local List and the UNSC Consolidated List and prevent access or use of funds or other assets that may be subject to freezing measures.

If the Reporting Entity does not conduct any business activities or transactions and where customers do not have access to any assets or accounts during weekends or holidays, then the screening obligation starts from the first minute of commencement of business and freezing measures must be applied immediately. In any case,
Company is ensuring that funds or other assets subject to TFS measures are prevented from being accessed or used.

12.10.) Implement TFS Measures

1. Freeze all funds or other assets without delay.
Freeze without delay (immediately or in any case within 24 hours) and without prior notice to the designated individual, entity, or group, all the funds or other assets:

a) Owned or controlled, wholly or jointly, directly, or indirectly, by an individual, entity, or group designated in the Local Terrorist List or the UN Consolidated List.
b) Derived or generated from funds or other assets under item (a); or
c) Any individual or entity acting on behalf of or at the direction of any designated individual, entity, or group.

2. Prohibition of making funds or other assets or services available
Entities are prohibited from providing funds or other assets to or rendering financial services or other services related to, whether in whole or in part, directly or indirectly, or for the benefit of any designated individual, entity, or group on the Sanctions List.

12.11.) REPORT

The mechanism to report any TFS measures taken upon identifying a Confirmed or Partial Name Match is through submitting one of the following two reports via goAML:

- Confirmed Name Match Report (CNMR)
- Partial Name Match Report (PNMR)

<u>Confirmed Name Match Report (CNMR)</u>

<u>Existing Customer:</u>

In case a **Confirmed Name Match** is identified on an existing customer, the Reporting Entity must freeze without delay (within 24 hours) and prohibit making funds or other assets or services available and submit a **CNMR** through goAML within five business days of implementing the freezing measures.

<u>Potential Customer / Counterparty</u>:

In case a Confirmed Name Match is identified on a potential customer (a prospective client) or counterparty of an existing customer in a transaction, the Reporting Entity must reject the transaction and refrain from dealing with or providing any funds or other assets or services to the Confirmed Name Match and submit a CNMR through goAML within five business days of rejecting the transaction. The report should clarify the actions taken by the Reporting Entity (rejected business relation or transaction), as well as any funds or other assets frozen in the process.

The following information is obligatory and must be provided (attached) when submitting a CNMR:

- **The full name of the 'Confirmed Name Match'**. Attach ID documents of the 'Confirmed Name Match', such as passport or ID card for individuals, and trade licenses and articles of association for entities. In cases of a Confirmed Name Match, it is assumed that the Reporting Entity possesses the ID documents of the confirmed match, **since verifying the confirmed match result without an ID is improbable and unlikely.**
- **Amount of funds or other assets frozen** – (e.g., value of funds in bank accounts, value of transactions, value of securities, value of real estate, etc.). Attach documentary proof to bank statements, transaction receipts, securities portfolio summary, title deeds, insurance policy, etc.
- **Description of rejected transaction or service –** (e.g. in case no funds are being held, and the transaction is service based, provide a description of the transaction / service rejected.)

<u>Partial Name Match Report (PNMR)</u>

<u>Existing Customer:</u>

In case a partial name match is identified on an **existing customer**, the Company is required to suspend without delay any transaction, refrain from offering any funds, other assets or services, and submit a Partial Name Match Report (PNMR) through goAML within **five business days** from suspension measures.
The Company must ensure all the necessary information and documents regarding the name match are submitted and maintain suspension measures related to the partial name match until further instructions are received from EOCN via goAML on whether to cancel the suspension (false positive') or implement freezing measures (confirmed match').

<u>Potential Customer / Counterparty:</u>

In case a **Partial Name Match** is identified on a **potential customer** (a prospective client) or a counterparty (supplier or customer), the company must make necessary efforts to obtain identification documents of the potential customer or counterparty to conclude whether the match is a Confirmed Name Match or False Positive. If, after obtaining the ID documents, company is able to conclude the result as a False Positive, then it may establish the business relation or allow the transaction to proceed without the need to report a PNMR; however, internal documentation of the False Positive result should be maintained.

If the company is unable to obtain the identification documents within a reasonable time (10 business days) of identifying the Partial Name Match, then the transaction or service should be rejected (cancelled) and a PNMR submitted through goAML within five business days from rejection of the transaction or service, specifying that the transaction has been rejected due to lack of ID documents of the Partial Name Match.

If the company receives the ID document of the potential customer or counterparty after the transaction has been rejected due to lack of ID document (i.e. reasonable period has passed – 10 business days) and the PNMR reported, it must conduct screening based on the newly obtained ID documents and take the necessary steps required depending on the screening result (Confirmed Name Match, False Positive, or unable to verify based on the provided ID documents). In this case, company may treat the case as a new transaction and submit a new report based on the screening results.

The following information is obligatory when submitting a PNMR:

- The full name of the ‘partial name match’. Attach ID documents of the ‘partial name match’, such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.

- Amount of funds or other assets suspended (e.g., value of funds in bank accounts, value of transactions, value of securities, value of real estate, etc.). Attach documentary proof such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.
- Description of rejected transaction or service – (e.g. in case no funds are being held, and the transaction is service based, provide a description of the transaction /service rejected.)

Reporting TFS by Email:

For non goAML users (Persons that do not fall under the definition of Reporting Entities – Fis, DNFBPs, and VASPs – and are therefore not under an obligation to register on goAML – these include all natural and legal persons in the UAE), the reporting of any freezing measures or attempted transaction by a designated individual, entity, or group must be communicated directly by email to the EOCN through tfs@eocn.gov.ae within five business days from implementing any freezing measures.

Non-Compliance

- ➢ Violating UAE Cabinet Decision No. 74 of 2020 can expose the Company to administrative penalties and criminal prosecutions including:

- Increased scrutiny of future actions from the UAE Government.
- Supervisory authority may determine a ban of certain individuals from employment within the relevant sectors for a period of time.
- A suspension, restriction, or prohibition of activity, business, or profession causing either revocation or withdrawal of the business license.

- ➢ Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing

- Every natural or legal person shall immediately comply with the instructions issued by the Competent Authorities in the State concerning the implementation of the resolutions issued by the UN Security Council.

12.12. SAMPLE TFS REPORTING TEMPLATES

12.12.1 SAMPLE CONFIRMED NAME MATCH REPORT (CNMR) – INTERNAL TEMPLATE

Title: Confirmed Name Match Report (CNMR)
Purpose: To document a confirmed match with the UAE Local Terrorist List or the UNSC Consolidated List and record all actions taken by AL RAFIDAIN JEWELLERY TRADING LLC in accordance with Cabinet Decision No. 74 of 2020.

A. Report Information

1. Date of Report:

2. Reporting Entity Name:

B. Details of the Confirmed Match

- Full Name (as per sanctions list):
- Date of Birth:
- Nationality:
- Passport/ID Number:
- Reason for Confirmation:
  All identifiers matched the UAE Local Terrorist List / UNSC Consolidated List during sanctions screening.

C. Customer Classification

- Existing Customer
- Potential Customer / Counterparty

D. Actions Taken

- Confirmed name match identified during sanctions screening.
- All funds or other assets were frozen without delay (within 24 hours), in line with UAE TFS requirements.
- No financial, commercial, or non-financial services were provided following identification.
- Customer or counterparty was not informed to avoid tipping off.
- Compliance Officer notified internally.

E. Details of Funds/Assets Frozen

- **Type of Funds/Assets:** (e.g., pending payment, gold items, account balance)
- **Total Value Frozen:**
- **Supporting Documents Attached:**
  - Customer identification documents
  - Transaction records/invoices
  - Asset valuation/receipts
  - Internal freezing confirmation

F. Description of Rejected or Blocked Transaction (if applicable)

[Brief description of attempted or ongoing transaction stopped due to confirmed match]

G. Reporting to FIU

A Confirmed Name Match Report (CNMR) will be submitted via goAML within five (5) business days of implementing freezing measures.

H. Report Prepared By

Name: _________________________
Position: ______________________
Signature: _____________________
Date: __________________________

12.12.2 SAMPLE PARTIAL NAME MATCH REPORT (PNMR) – INTERNAL TEMPLATE

Title: Partial Name Match Report (PNMR)
Purpose: To document a partial or potential match identified during sanctions screening and actions taken pending verification or guidance from EOCN.

A. Report Information

1. Date of Report:

2. Reporting Entity Name:

B. Details of Potential Match

- Name Causing Partial Match:
- Identifiers Triggering Match:
  (e.g., similar spelling, close phonetic match, shared surname)

C. Customer Classification

- Existing Customer
- Potential Customer / Counterparty

D. Actions Taken

- Transaction suspended without delay pending verification.
- No funds, assets, or services were provided.
- Customer/counterparty was not informed to avoid tipping off.
- Attempts were initiated to obtain identification documents for verification.

E. Information Obtained for Verification

- Customer ID/passport
- Trade license/Articles of Association (for entities)
- Any additional documentation obtained

F. Current Status of the Match

- Verified as False Positive (no PNMR required; documented internally)
- Unable to verify – PNMR will be filed; transaction rejected
- Partial indicators remain – PNMR will be submitted and suspension continues pending EOCN instruction

G. Details of Suspended/Revised/Rejected Transaction

- Nature of Transaction:
- Value of Suspended Assets/Funds:
- Supporting Documents: (invoices, purchase orders, receipts, etc.)

H. Reporting to FIU

A Partial Name Match Report (PNMR) will be submitted via goAML within five (5) business days of the suspension or rejection.

I. Report Prepared By

Name: ________________________
Position: _____________________
Signature: _____________________
Date: _________________________

13. INTERNAL CONTROLS

- The Company has the appropriate internal controls to ensure compliance with the most recent publication of targeted financial sanctions on the UNSC Consolidated lists and the Local Lists.

- The Company is having the Internal controls and procedures to ensure compliance with the obligations arising from Cabinet Resolution 74/2020.

- The Company has implemented Policies and procedures that prohibit staff from, directly or indirectly, informing the customer or any third party that freezing action or any Other Measures as per provisions of Cabinet Resolution 74/2020.

- Identify the existing accounts, transactions, funds or other assets of designated individuals, entities, or groups.

- Conduct ongoing TFS training and awareness sessions for relevant employees and senior management.

- Adopt reasonable measures to consider beneficial owners, signatories, and powers of attorney with respect to accounts or transactions when searching for activities by designated individuals, entities, or groups.

14. NEW TECHNOLOGIES AND VIRTUAL ASSETS (VA)

The Company is aware that Federal Decree-Law No. 10 of 2025 and its Executive Regulations explicitly cover Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs).

The Company has determined that dealing in Virtual Assets (VAs), including but not limited to cryptocurrencies, stablecoins, or Non-Fungible Tokens (NFTs), presents a high inherent risk for Money Laundering and Proliferation Financing, given the nature of its business as a Dealer in Precious Metals and Stones (DPMS).

As a mandatory, definitive internal control, the Company strictly prohibits the acceptance of any form of Virtual Asset as payment for goods or services.

Any attempt by a customer to transact using a Virtual Asset must be:

1. Rejected: immediately by the employee.
2. Documented: as a high-risk red flag in the customer's file.
3. Escalated: immediately to the Compliance Officer/MLRO.
4. Considered: for the filing of a Suspicious Transaction Report (STR) based on the attempted use of an illicit or prohibited payment method.

15. HIGHLIGHTS OF KEY PROVISIONS AFFECTING THE COMPANY

The AML-CFT Law and the AML-CFT Decision contain numerous provisions setting out the rights and obligations of the Company as well as their senior managers and employees. This section highlights some of the key provisions affecting the Companies that are of immediate concern. The Company reminded that it is their sole responsibility to adhere to all provisions of the AML-CFT Law, the AML-CFT Decision, and all regulatory notices, rulings and circulars affecting them.

15.1. SUMMARY OF MINIMUM STATUTORY OBLIGATIONS OF THE COMPANY

The AML-CFT Law and the AML-CFT Decision set out the minimum statutory obligations of the Company as follows:

- To identify, assess, understand risks.
- To define the scope of and take necessary due diligence measures.
- To appoint a compliance officer, with relevant qualification and expertise and in line with the requirements of the relevant Supervisory Authority.
- To put in place adequate management and information systems, internal controls, policies, procedures to mitigate risks and monitor implementation.
- To put in place indicators to identify suspicious transactions.
- To report suspicious activity and cooperate with Competent Authorities.
- To maintain adequate records.

15.2. CONFIDENTIALITY AND DATA PROTECTION

The Company is obliged to report to the UAE's Financial Intelligence Unit (FIU) when they have reasonable grounds to suspect a transaction or funds representing all or some proceeds, or suspicion of their relationship to a Crime. In reporting the suspicions, we must maintain confidentiality with regard to both the information being reported and to the act of reporting itself and make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

The confidentiality requirement does not pertain to communication within the Company 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 a Crime. However, under no circumstances does the Company, or their managers or employees permit to inform a customer or the representative of a Business Relationship, either directly or indirectly, that a report has been made under penalty of sanctions. This is the so-called "tipping off" requirement. This also extends to any related information that might be provided to the FIU or information that is being requested by the FIU.

The Company is not permitted to object to the statutory reporting of suspicions on the grounds of Customer confidentiality or data privacy, under penalty of sanctions. Moreover, data protection laws include provisions that allow the Company to report to the authorities.

15.3. PROTECTION AGAINST LIABILITY FOR REPORTING PERSONS

(AML-CFT Law Article 27; AML-CFT Decision Article 17.3)

The Company as well as their members, employees and authorized representatives, are protected by the relevant articles of the AML-CFT Law and AML-CFT Decision from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This is also the case even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. However, it should be noted that such protections do not extend to the unlawful disclosure of the customer or any other person, whether directly or indirectly, that they have reported or intended to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

15.4. STATUTORY PROHIBITIONS

(AML-CFT Law Article 16.1(c); AML-CFT Decision Articles 13.1, 14, 35.4, 38)

The Company is prohibited from the following activities:

- Establishing or maintaining any Customer or Business Relationship, conducting any financial or commercial transactions, keeping any Business Relationship under an anonymous or fictitious name or by pseudonym or number.

- Establishing or maintaining a Business Relationship or executing any business dealing in the event they are unable to complete adequate risk-based CDD measures in respect of the Customer for any reason.

- Dealing in any way with Shell Banks, whether to open accounts with the Company or to facilitate any banking transactions for themselves or on behalf of the customers.

- Invoking banking, professional or contractual secrecy as a pretext for refusing to perform statutory reporting obligation in regard to suspicious activity.

- Facilitating issuance of bearer shares or bearer share warrants.

15.5. MONEY LAUNDERING

Money laundering is any act involving the transfer, conversion, concealment, acquisition, possession, use or handling of funds or other property, by any means, with the knowledge or a reasonable belief that such funds or property are the proceeds of a crime, or with the intention of disguising or misrepresenting their unlawful origin, assisting any person involved in committing the predicate offence to evade legal consequences, or obstructing the identification, tracing, freezing, seizure or confiscation of such funds or property. The offence of money laundering is independent from the predicate offence and may be established on the basis of inferences drawn from objective facts and surrounding circumstances, without requiring direct evidence of actual knowledge on the part of the offender, in line with Federal Decree-Law No. 10 of 2025.

Money laundering may be committed through any channel, including traditional financial systems, digital systems, virtual assets, encryption technologies, or trade-based mechanisms. The Company treats any transaction, customer behavior, or pattern that raises reasonable suspicion of involvement in such activities as requiring immediate escalation and potential reporting, regardless of the specific method or technology used.

15.6. PREDICATE OFFENCES

Predicate offences are all crimes designated under the laws of the United Arab Emirates that generate proceeds capable of being laundered, including but not limited to fraud, bribery and corruption, embezzlement, theft, forgery, smuggling, environmental crimes, cyber-enabled crimes, tax-related offences, financing of terrorism and illegal organisations, trafficking in narcotic drugs and psychotropic substances, human trafficking, and the financing of proliferation of weapons, including arms proliferation. For the purposes of this Policy, any suspicion that funds or property are derived from any such offence, whether committed inside or outside the State, shall be treated as a predicate offence for money laundering.

The list of predicate offences under Federal Decree-Law No. 10 of 2025 is comprehensive and continuously updated by competent authorities. The Company shall treat any transaction, customer, or activity where there is reasonable suspicion of connection to predicate offences as requiring enhanced scrutiny, documentation, and potential suspicious transaction reporting, regardless of whether the specific predicate offence can be identified with certainty.

15.7. TERRORISM FINANCING

An offense within the meaning of the UN International Convention for the Suppression of the Financing of Terrorism (1999), where a person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

- An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex of the above-mentioned treaty, or
- Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing an act.

(AML-CFT Law Articles 3.1, 4, 29.3, AML-CFT Decision Article 1)

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

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organization or terrorist person or intended to finance a terrorist organization, a terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin; or

- Providing, collecting, preparing or obtaining proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or committing such acts on behalf of a terrorist organization or a terrorist person while aware of their true background or purpose.
  In a 2019 report by MENAFATF, an assessment of the global threat posed by the financing of terrorism stated.
  “The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified considerably. In addition to the threat posed by terrorist organizations such as ISIL, Al-Qaeda and other groups, attacks in many cities across the globe are carried out by individual terrorists and terrorist cells ranging in size and complexity. Commensurate with the evolving nature of global terrorism, the methods used by terrorist groups and individual terrorists to fulfil their basic need to generate and manage funds is also evolving.
  Terrorist organization’s use funds for operations (terrorist attacks and pre-operational surveillance); propaganda and recruitment; training; salaries and member compensation; and social services. These financial requirements are usually high for large terrorist organizations, particularly those that aim to, or do, control territory. In contrast, the financial requirements of individual terrorists or small cells are much lower with funds primarily used to carry out attacks. Irrespective of the differences between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist groups and individual terrorists seek to ensure adequate funds generation and management.

15.8. FINANCING OF ILLEGAL ORGANISATIONS

(AML-CFT Law Articles 3.2, 4, 29.3, AML-CFT Decision Article 1)
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 the risk exposure to the financing of illegal organizations, the Company is placing significant emphasis on 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.

16. PROLIFERATION AND PROLIFERATION FINANCING

Proliferation Financing (PF), including Financing of Arms Proliferation, is a standalone principal offence and predicate offence to money laundering under Federal Decree-Law No. 10 of 2025, encompassing the raising, moving, or provision of funds/assets for weapons of mass destruction (WMD), their means of delivery, or related dual-use goods/technologies.

AL RAFIDAIN JEWELLERY TRADING LLC integrates PF risks into all controls, including Customer Risk Assessment (CRA), Enterprise-Wide Risk Assessment (EWRA), Customer Due Diligence (CDD)/Enhanced Due Diligence (EDD), transaction monitoring, red flag indicators, and STR/SAR filing.

PF Risk Indicators for DPMS:
• Customers/counterparties linked to dual-use goods, high-risk PF jurisdictions (e.g., FATF grey/black lists), unusual trade routes, or WMD-related sectors (nuclear/chemical/biological).
• Transactions involving commodities subject to non-proliferation controls under Federal Decree-Law No. 43 of 2021 or UNSCRs 1718/2231.
• Complex ownership structures, front companies, or procurement patterns inconsistent with legitimate PMS trade.

17. THE MONEY LAUNDERING PHASES

The Company is fully aware of the three phases of money laundering. By determining for which ML/FT phase a certain product can be misused, or the Company itself can be misused, it will help the Company understand its specific inherent ML/FT risks. The paragraphs below describe the crime of money laundering as consisting of three distinct phases:

Placement.

In this phase, criminals attempt to introduce Funds or the Proceeds of Crime into the financial system using a variety of techniques or typologies.

Examples of placement transactions include the following:

- ✓ Blending of funds: Commingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned businesses.
- ✓ Foreign exchange: Purchasing foreign exchange with illegal funds.
- ✓ Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade attention or reporting requirements.
- ✓ Currency smuggling: Cross-border physical movement of cash or monetary instruments.
- ✓ Loans: Repayment of legitimate loans using laundered cash.

Layering

Once the Funds or Proceeds are introduced, or placed into the financial system, they can proceed to the next phase of the process; often, this is accomplished by placing the funds into circulation through formal financial institutions, and other legitimate businesses, both domestic and international. In this layering phase, criminals attempt to disguise the illicit nature of the Funds or Proceeds of Crime by engaging in transactions, or layers of transactions, which aim to conceal their origin.

Examples of layering transactions include:

- ✓ Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets.
- ✓ Moving funds from one financial institution to another or within accounts at the same institution;
- ✓ Converting the cash placed into monetary instruments;
- ✓ Reselling high-value goods and prepaid access/stored value products;
- ✓ Investing in real estate and other legitimate businesses;
- ✓ Placing money in stocks, bonds or life insurance products; and
- ✓ Using shell companies to obscure the ultimate beneficial owner and assets.

Integration

In this phase, criminals attempt to return, or integrate, their “laundered” Funds or the Proceeds of Crime back into the economy, or to use it to commit new criminal offences, through transactions or activities that appear to be legitimate.

A key objective for criminals engaged in money laundering—and therefore a key generic risk underlying the specific risks faced by the Company—is the exploitation of situations and factors (including products, services, structures, transactions, and geographic locations) which favor anonymity and complexity, thereby facilitating a break in the “paper trail” and concealment of the illicit source of the Funds.

The Company is diligently ensuring that the business is not utilized, either directly or indirectly, to facilitate money laundering or the financing of terrorism or illegal organizations in any of the three stages.

17.1. ML/FT TYPOLOGIES

The methods used by criminals for money laundering, the financing of terrorism, and the financing of illegal organizations are continually evolving and becoming more sophisticated. Moreover, the variety of transactions and activity types involving DPMS can be very wide. It is

therefore impossible to provide an exhaustive list of ML/FT typologies for DPMS, as new typologies and techniques are constantly being developed and attempted.
Nevertheless, research on the subject and analysis of case studies from around the world has identified some common methods used by criminals for the purposes of ML/FT involving DPMS. These methods broadly align with the classical stages of the ML/FT process i.e. placement, layering, and integration; however, they can also involve PMS as a vehicle for committing a predicate offence, or as the direct proceeds of crime
The following have been identified as being amongst the common typologies used for exploiting DPMS for the purpose of ML/FT, according to the Financial Action Task Force (FATF):

- Use of PMS as an alternative to currency.
- PMS as stored value instruments/means to realize the proceeds of crime
- Laundering illegal PMS and/or the use of PMS to launder the proceeds of crime.
- Trade-based ML.
- Physical smuggling of PMS.

18. SANCTIONS AGAINST PERSONS VIOLATING REPORTING OBLIGATIONS

(AML-CFT Law Articles 15, 24, 25)
The AML-CFT Law provides for the following sanctions against the Company, managers or employees, who fail to perform, whether purposely or through gross negligence, their statutory obligation to report a suspicion of money laundering or the financing of terrorism or of illegal organizations:

- ✓ Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or

- ✓ Any of these two sanctions.

According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a Crime. It should also be noted that the transactions or funds that are the subject of the suspicion may represent only part of the proceeds of the criminal offence, regardless of their value Likewise, the AML-CFT Law provides for sanctions against anyone who warns or notifies a person of a suspicious transaction report or reveals that a transaction is under review or investigation by the Competent Authorities, as follows:

- ✓ Imprisonment for no less than six months and a penalty of no less than AED100,000 and no more than AED 500,000; or
- ✓ Any of these two sanctions.

19. CUSTOMER RISK ASSESSMENT (CRA)

The Company is committed to identifying, assessing, and understanding the Money Laundering (ML), Terrorism Financing (TF), and Proliferation Financing (PF) risks associated with our

clients in accordance with the UAE's AML/CFT Law, its by-laws, and the Ministry of Economy's (MOE) AML/CFT Guidelines for Designated Non-Financial Businesses and Professions.
The customer risk assessment focuses on evaluating the risk that natural person or legal entity clients present in relation to ML/TF/PF. The CRA's include identifying high-risk clients, adjusting monitoring and due diligence procedures accordingly, and mitigating specific risks associated with them. This involves analyzing customer characteristics, behaviors, transaction patterns, and geographic risks to assess the likelihood of involvement in financial crimes. This assessment helps determine the appropriate level of due diligence and monitoring required, especially during customer onboarding and periodic reviews.
The Company implemented LiveEx Shield AML Software for the risk assessment procedures based on the NRA – National Risk Assessment guidance and sector-specific requirements.

19.1 CRA IMPLEMENTATION

19.1.1 RISK FACTORS

- Customer Risk;
- Geographic Risk;
- Product/Services Risk;
- Transaction Risk; and
- Delivery Channel Risk.

Proliferation Financing (PF) Risk Factors

- Customers or counterparties linked to dual-use goods, high-risk PF jurisdictions, unusual trade routes, or WMD-related sectors (such as nuclear, chemical, or biological industries).
- Transactions involving commodities or activities that may be subject to non-proliferation controls, including those covered by Federal Decree-Law No. 43 of 2021 and relevant UN Security Council Resolutions.
- Complex ownership structures, front companies, or procurement patterns that are inconsistent with the customer's stated business profile or with legitimate precious metals and stones trade (see Section 15 for further details).

The Company currently does not provide, mediate, accept payments via, or engage with Virtual Assets (VAs) or Virtual Asset Service Providers (VASPs). Any future involvement requires prior AML/CFT/PF risk assessment, Board approval, and enhanced controls. Customers requesting settlement via third-party/personal accounts unrelated to their verified business profile, or via VAs/VASPs, shall be classified as high-risk, subject to Enhanced Due Diligence (EDD), Source of Funds/Source of Wealth verification, and potential Suspicious Transaction Report (STR) filing.

19.1.2 RISK LEVELS, REQUIRED ACTIONS, AND REVIEW PERIOD

- 0-1 - Low Risk
- 1.1-2 - Low-Medium Risk
- 2.1-3 Medium Risk
- 3.1-4 Medium-High Risk

- 4.1-5 High Risk

Risk Category	Action Required	Risk Controls	Risk Score	Review Period
Low	Simplified CDD – Customer Due Diligence	Customer Identity Documents Collection, Sanction Screening verification, and Risk Assessment.	1	2 years
Low-Medium	CDD – Customer Due Diligence	Customer Identity Documents Collection, Sanction Screening verification, and Risk Assessment.	2	Every 1.5 years
Medium	Enhanced CDD – Enhanced Customer Due Diligence	Customer Identity Documents Collection, Sanction Screening Verification, Customer Risk Assessment and Transaction Purpose.	3	Every 1 year
Medium-High	EDD – Enhanced Customer Due Diligence	Customer Identity Documents Collection, Sanction Screening Verification, Customer Risk Assessment, Transaction Purpose, Source of Fund and documents support (i.e., BLs/AWs, Invoices, Transport Docs).	4	Every 1 year
High	EDD – Enhanced Customer Due Diligence	Customer Identity Documents Collection, Sanction Screening Verification, Customer Risk Assessment, Transaction Purpose, Source of Fund and documents support (i.e., BLs/AWs, Invoices, Transport Docs).	5	Every 6 months

19.2 RISK MATRIX

Total Sum of Risk (Customer + Relation) / Total No. of Risk = Customer Risk
Customer Risk * Mitigation Risk = Residual Risk

19.3 COLLECTING INFORMATION AND DOCUMENTS

The Company implements the CDD process to verify customer identities, source of funds, business activities, and all transaction-related information and documentation.

19.4 ASSESSING CUSTOMER RISK

The Company classifies customers into risk categories based on identified factors using a completed risk matrix within its risk scoring system.

19.5 CALCULATE OVERALL RISK SCORE

The Company calculates an overall risk score by averaging the scores from each risk factor.

19.6 CONTROLS

For high-risk scenarios, the Company conducts Enhanced Due Diligence (EDD) to gain a deeper understanding of their profile, financial activities, and potential risks. This includes obtaining additional identification documents, verifying the source of funds, assessing the nature and purpose of the business relationship, and conducting more frequent monitoring of transactions and their profile.
As per the AML/CFT/TFS requirements the Company is required to:

- Identify, assess, monitor, manage and take effective action to mitigate ML/TF risks using a risk-based approach that requires enhanced measures when risks are higher.
- Carry out Customer Due Diligence (CDD) with respect to the customer, beneficial ownership, and business relationship either themselves and/or with reliance on third parties that fulfil specific criteria.
- Take additional measures and precautions for politically exposed persons (PEPs).
- Maintain records on CDD information and transactions.
- Identify, assess, manage, and mitigate ML/ TF risks that arise when developing new products, business practices, or delivery channels or when using or developing modern technologies.
- Implement policies, procedures, and internal controls against ML/TF risks.
- Apply enhanced due diligence (EDD) when dealing with customers or entities from high risk and sanctioned countries.
- Report suspicious activities & transactions to the financial intelligence unit (FIU). DNFBPs should be protected by law from criminal and civil liability for the breach of any confidentiality clause made in this regard. Note that lawyers, notaries, other independent professionals & accountants are not required to report suspicious activities if the information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
- Not tip off clients when an STR is filed with the FIU. Tipping off should be prohibited by law.
- Have access to and share information on beneficial ownership and control of legal persons & arrangements.
- Provide records and information to competent authorities to aid in ML/TF investigations carried out by them, or as a consequence of mutual legal assistance (MLA) requests.

19.7 RISK-BASED APPROACH (RBA):

- The Company shall conduct a formal ML/TF/PF Risk Assessment in accordance with Article 4 of Federal Decree-Law No. 10 of 2025, including:
- Risk identification of customers, jurisdictions, products/services, delivery channels and supply chain actors.
- Risk assessment using a documented methodology.
- Risk mitigation tailored to identified risks.
- Annual review approved by Senior Management.
- Reassessment upon introduction of new business lines or emerging risks.

20. ENTERPRISE-WIDE ML/TF/CPF RISK ASSESSMENT (EWRA)

In accordance with Article 4 of Federal Decree-Law No. 10 of 2025, the Company shall conduct a formal, documented, and comprehensive Money Laundering, Terrorism Financing, and Proliferation Financing (ML/TF/PF) Assessment. This assessment shall be carried out at least annually and whenever there is a material change in the Company’s products, services, customer base, delivery channels, jurisdictions, or business operations.

Proliferation Financing (PF) risk shall be assessed as a separate and independent risk category in the EWRA, in line with Federal Decree-Law No. 10 of 2025.”

The assessment shall include:

• Identification of ML/TF/PF risks

• Analysis and evaluation of risks using a documented methodology

• Application of risk-based mitigation controls

• Approval by Senior Management

• Maintenance of records to demonstrate implementation and effectiveness.

This assessment constitutes the enterprise-wide ML/TF/PF risk assessment (EWRA) required by Federal Decree-Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025. The Institutional Risk Assessment (IRA) evaluates the Company's overall exposure to ML/TF/PF risks, including proliferation financing (PF) and sanctions evasion, considering industry-specific risks (DPMS high-risk sector per UAE NRA), operational processes, internal policies, regulatory compliance, virtual assets exposure (currently none), new delivery channels/technologies, and effectiveness of existing AML/CFT/CPF controls. The EWRA/IRA shall be approved and reviewed by the Board/senior management at least annually and upon material changes in products, business practices, geographic exposure, or regulatory requirements, with results tabled at Board meetings.

PF risks are assessed per Section 15 and integrated into overall EWRA scoring, with specific consideration of supply chain vulnerabilities, dual-use goods exposure, EOCN/TFS lists, and DPMS-specific proliferation financing risks identified in the UAE National Risk Assessment (NRA) 2024 and MoE guidance.

1. Risk Identification

The Risk Assessment shall identify inherent risks related to:

- Customer types and profiles
- Jurisdictions and geographic exposure
- Products and services
- Delivery channels
- Transactions and payment methods
- Supply-chain actors including miners, refiners, and intermediaries
- New technologies and business processes

2. Documented Methodology

The Company shall use a consistent and documented methodology including:

- Risk scoring criteria
- Weighting allocation for each risk category
- Inherent and residual risk ratings
- Evidence-based justification for ratings

3. Risk Mitigation

Mitigation measures shall be aligned with the identified risks, such as:

- Enhanced Due Diligence for high-risk customers
- Heightened monitoring
- Senior Management approvals
- Rejection of high-risk customers where risks cannot be mitigated

4. Annual Review

The Risk Assessment shall be:

- Reviewed at least annually, or earlier if major changes occur
- Approved by Senior Management
- Made available to Competent Authorities upon request

20.1. AL RAFIDAIN JEWELLERY TRADING LLC– RISK ASSESSMENT FORM

The purpose of an ML-TF-PF (Money Laundering, Terrorist Financing, & Proliferation Financing) Risk Assessment Form is to evaluate and assess the level of ML-TF-PF risk associated with various entities, activities, or transactions within an organization or industry. It provides a systematic approach to identify, measure, and manage the risks related to money laundering and terrorist financing.

The ML-TF-PF Risk Assessment Form typically includes the following elements:

Risk Identification: The form helps in identifying and documenting the specific ML-TF-PF risks that are relevant to the organization or industry. This involves considering various factors such as customer types, geographical locations, product or service offerings, transaction volumes, and other relevant risk indicators.

Risk Assessment: The form enables the evaluation and scoring of ML-TF-PF risks based on their severity and likelihood of occurrence. It may utilize a scoring system or other metrics to quantify and compare the risks. This assessment provides a quantitative basis for prioritizing and addressing the identified ML-TF-PF risks.

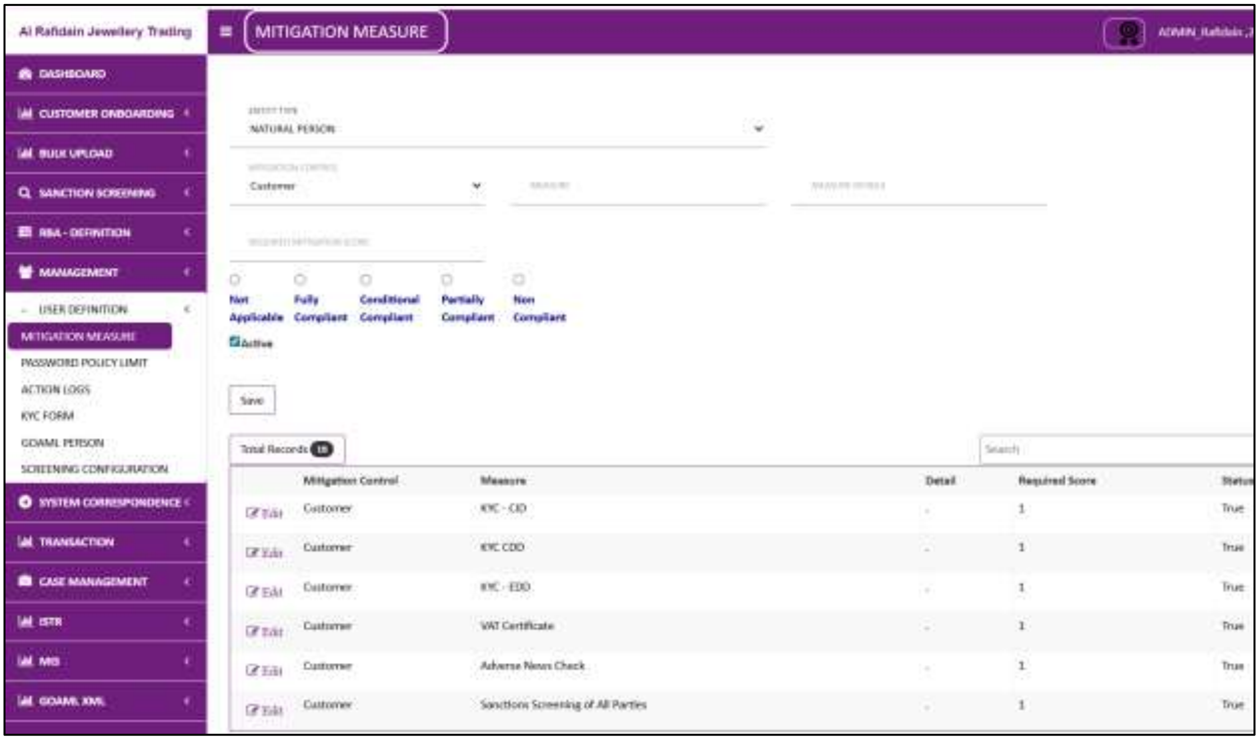
Risk Mitigation Strategies: The form outlines the strategies and controls that will be implemented to mitigate the identified ML-TF risks. These strategies may include customer due diligence measures, transaction monitoring systems, training programs, internal controls, and other risk mitigation measures specific to ML-TF-PF.

Responsible Parties: The form assigns responsibilities to individuals or teams responsible for implementing the risk mitigation strategies and ensuring compliance with Anti-Money Laundering and Counter-Terrorist Financing and Proliferation Financing regulations. This ensures accountability and clear ownership of the risk management process.

Resource Allocation: The form may include a section to document the resources required to implement risk mitigation strategies effectively. This may include financial resources, personnel, technology, or other necessary assets. Proper resource allocation ensures that adequate measures are in place to mitigate ML-TF-PF risks.

Monitoring and Review: The form may include provisions for ongoing monitoring and review of the implemented risk mitigation measures. This involves regular assessments of the effectiveness of the strategies, periodic reassessment of ML-TF-PF risks, and the identification of emerging risks or regulatory changes that may require adjustments to the risk mitigation approach.

Documentation and Reporting: The form serves as a central repository for documenting the ML-TF-PF risk assessment and mitigation efforts. It provides a record of the risks identified, mitigation strategies implemented, responsible parties, resource allocation, and monitoring outcomes. This documentation is crucial for internal reporting, audit purposes, and compliance with regulatory requirements.

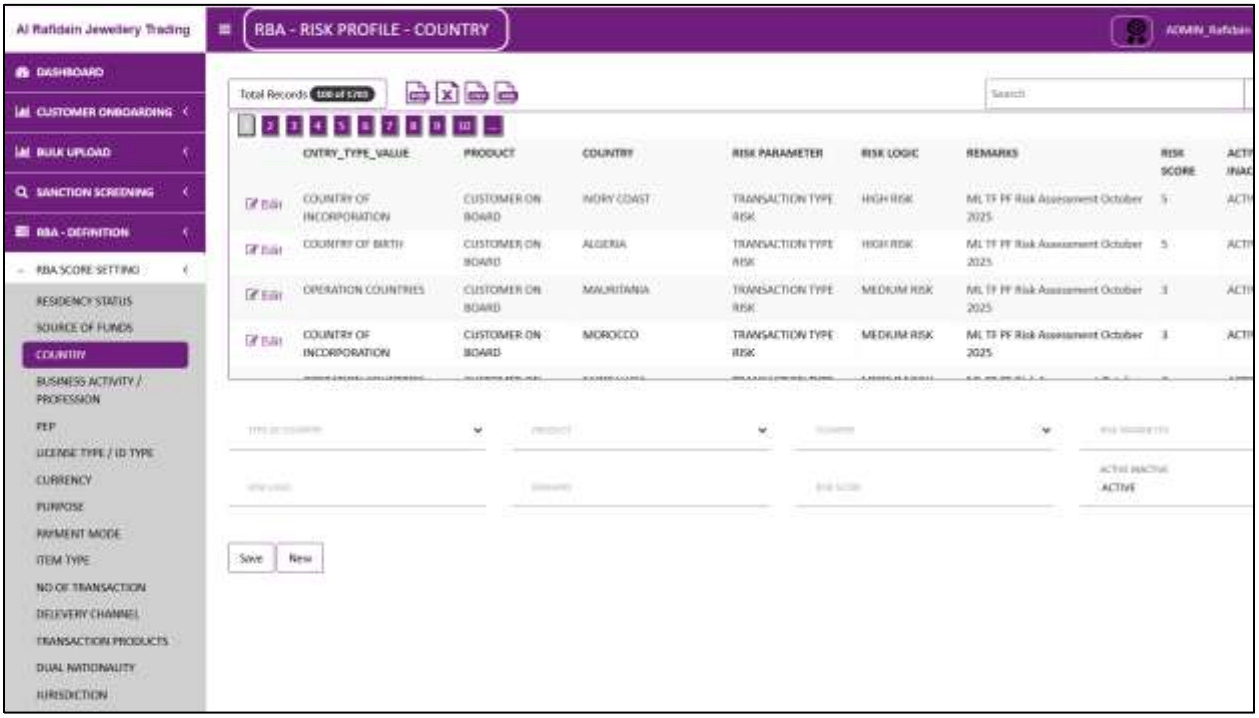


Note: Risk Mitigation Form is a tool used to systematically plan, track, and document the actions taken to address identified risks within an organization. It helps ensure that risk mitigation efforts are structured, accountable, and effectively implemented, ultimately reducing the organization's exposure to potential risks.

20.2. RISK ASSESSMENT SCORE SETTING

The purpose of risk assessment score setting is to evaluate and quantify the level of risk associated with various activities, processes, or entities within an organization. It involves assigning numerical values or scores to different risk factors based on their likelihood and potential impact. The risk assessment scores provide a standardized method for comparing and prioritizing risks, allowing organizations to allocate resources effectively and implement appropriate risk mitigation strategies.

The risk assessment score setting serves as a valuable tool in risk management, enabling organizations to systematically identify, prioritize, and mitigate risks while effectively allocating resources. It enhances decision-making, supports proactive risk management practices, and promotes a comprehensive understanding of the risk landscape within an organization.



21. AML/CFT COMPLIANCE PROGRAM

The Pillars of our AML/CFT and Sanctions Compliance include:

- Appointment of a Compliance Officer
- Adherence to Sanctions Compliance
- Customer Risk Assessment
- Institutional Risk Assessment
- Undertaking Customer Due Diligence for all clients and Enhanced Due Diligence for High-Risk Clients and PEPs
- Dissemination of Suspicious Activity Indicators to employees
- Identification of Suspicious Activity and reporting of Suspicious activity to the Financial Intelligence Department through GOAML Portal
- Employee Screening and Staff Training
- Independent Review of AML/CFT Sanctions Compliance program
- Record-keeping

22. STATUTORY PROHIBITIONS

Company commits that we will not:

A. Establish or maintain any Customer or Business Relationship or conduct any financial or commercial transactions with any natural or legal person who is anonymous or known by fictitious name or by pseudonym or number.

B. Establish or maintain a Business Relationship or execute any transaction in the event we are unable to complete adequate risk-based CDD measures in respect of the Customer for any reason.

C. Deal with Customers listed under any Sanction watch list and/or United Nation's "Consolidated List" and UAE Local Terrorist list.

D. Invoke professional or contractual secrecy as a pretext for refusing to perform our statutory reporting obligation with respect to suspicious activity.

23. STEPS TAKEN BY AL RAFIDAIN JEWELLERY TRADING LLC

a) Registered in the Financial Intelligence Unit (GoAML) portal.
b) Implemented a sanction screening system.
c) Appointed a Compliance Officer
d) Conducts Due Diligence on clients by verifying the identity of customer and beneficial owner before establishing a business relationship or opening an account.
e) Ensures Compliance with sanctions screening and reports any suspicious activity.

Company will be reporting through online Go-AML portal provided by the FIU.
All reporting is to be done at the time of receiving the funds. Reporting to be done within 2 weeks of occurring the qualifying transactions.

24. AML COMPLIANCE PILLARS

25. FIRST LINE OF DEFENSE

Onboarding Function – Sales / Accountants / Employees responsible for onboarding the customer and collection of Customer/Clients Documentation.

26. SECOND LINE OF DEFENSE

Compliance Function – Responsible for approving onboarding of Customer/Clients after applying Risk Based Approach and ensuring proper due diligence of the customer. Performing Sanction Screening and keeping records of customer onboarding.

27. THIRD LINE OF DEFENSE

Internal Audit Function – Responsible to Audit the Compliance Framework adopted by the company and ensuring that the processes are implemented as per the AML/CFT Policies and Regulations issued for DNFBPs.

25. APPOINTMENT OF COMPLIANCE OFFICER

A dedicated compliance officer manages the AML & Compliance function of company. The Compliance Officer (CO) is responsible for implementation and oversight of organization's compliance with AML/CFT rules and regulations, staff training, etc.

The Company ensures that the Compliance Officer Shall:

- ✓ Be an Independent staff in the organization;
- ✓ Report directly to the owner, MOE and other competent authorities;
- ✓ Be provided with sufficient resources including time, systems, tools and support staff depending on the nature, size and complexity of its business;
- ✓ Be provided with unrestricted access to all information related to products or services, business partners, suppliers, correspondent agents, customers and transactions;

26. ROLES AND RESPONSIBILITIES OF COMPLIANCE OFFICER

- ✓ The Compliance Officer is in charge of reviewing, scrutinizing and reporting STRs.
- ✓ The Compliance Officer should ensure the quality, strength and effectiveness of the Organization's AML/CFT program.
- ✓ Establishing and maintaining AML/CFT policies and procedures.

- ✓ Ensuring that the organization complies with the applicable AML/CFT laws.
- ✓ Ensuring day-to-day compliance with own internal AML/CFT policies and procedures.
- ✓ Responding promptly to any reasonable request for information if made by the Competent Authorities.
- ✓ Acting as the main point of contact with respect to handling internal suspicious transactions reports from the employees and analyze them before reporting to FIU. He / She shall also be the main contact point for coordinating with FIU and other concerned bodies regarding AML / CFT.
- ✓ Submit the threshold (AED 55,000/-) Exceeded transactions on timely manner into the GoAML System.
- ✓ Submit Suspicious Transaction Reports to the FIU in a timely manner.
- ✓ The Compliance Officer is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organizations, for reporting suspicions to the FIU.
- ✓ Cooperate with and provide the FIU with all information it requires for fulfilling their obligations.
- ✓ The Compliance Officer is in charge of informing and reporting to senior management on the level of compliance and reporting on that to the relevant Supervisory Authority.
- ✓ Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML / CFT matters (whether internal or external) and developing AML Training calendar to ensure all staff are adequately trained.
- ✓ Conduct regular gap analysis on new notices/regulations/best practices issued by regulatory bodies vis-à-vis this AML Compliance policy.
- ✓ Ensure all key documents pertaining to KYC of customers, customer transactions and STR are retained for the minimum period of 5 years.
- ✓ The Compliance Officer is responsible for filing the STR in GoAML System and coordinating with regulators for further investigation process.
- ✓ Working with senior management and other internal and external stakeholders to ensure that the Company's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.

27. ROLES AND RESPONSIBILITIES OF THE OWNER

- ✓ The owner is the overall responsible for implementing the robust compliance program across each business product, counterparty, country in which it deals, delivery channel of its services, customers etc.
- ✓ The owner must ensure that the company has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- ✓ The owner approves the overall business risk assessment for the Company.
- ✓ The owner ensures that all employees of the organization are being trained on the AML/CFT.
- ✓ The owner reviews the compliance issues raised by the compliance department.
  Under the new AML law, owners and senior managers may be held personally liable where serious or systematic AML/CFT/CPF control failures occur with their knowledge or due to gross negligence.

28. SENIOR MANAGEMENT ACCOUNTABILITY

Senior management, including the Owner and Manager of AL RAFIDAIN JEWELLERY TRADING LLC, bear ultimate responsibility for the effective implementation of this AML/CFT/CPF/TFS Policy and compliance with Federal Decree-Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025. They are personally accountable for ensuring adequate resources, oversight, and risk mitigation, and may face individual liability, including fines or imprisonment, for failures in program oversight or breaches.

Senior management shall receive periodic AML/CFT/CPF/TFS reports at least quarterly or bi-annually, covering: Enterprise-Wide Risk Assessment (EWRA) updates, Customer Risk Assessment (CRA) trends, high-risk relationships, Suspicious Transaction Reports (STRs)/Suspicious Activity Reports (SARs), Proliferation Financing (PF) and Targeted Financial Sanctions (TFS) incidents, audit findings, and remediation actions. These reports must be documented, approved, and retained for supervisory review by the Ministry of Economy.

29. KNOW YOUR CUSTOMER – KYC

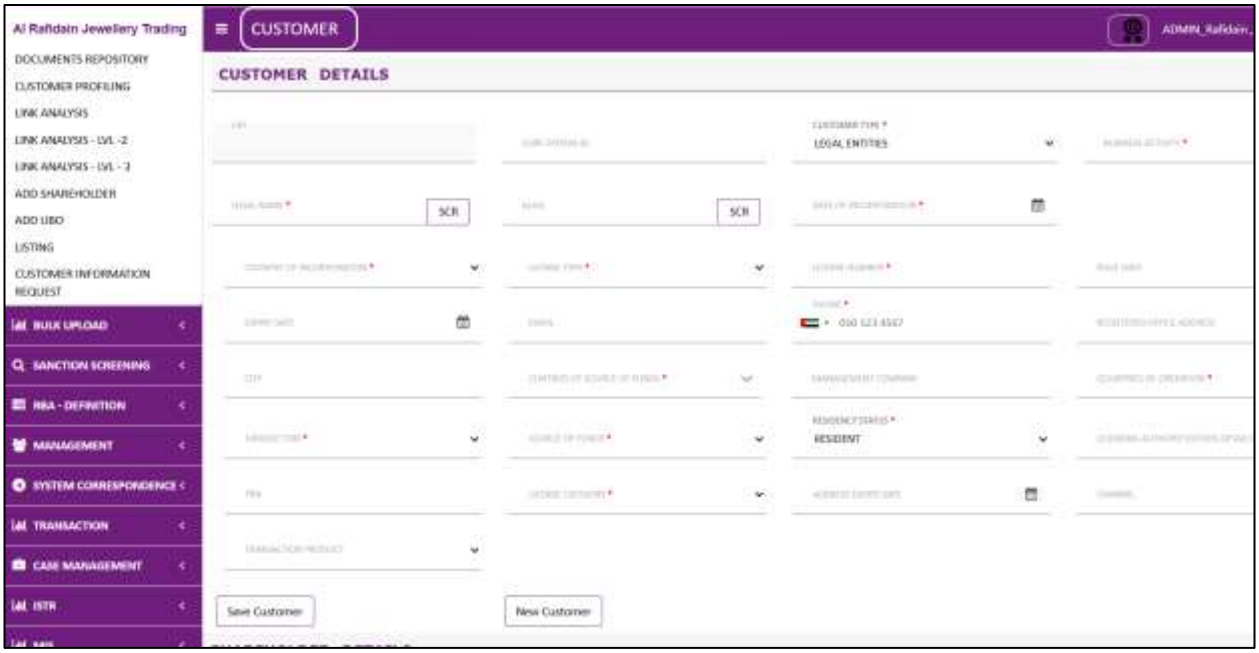
KYC is an acronym for "Know Your Customer" The foremost tool of Anti-Money Laundering / Combating Terrorism of Financing policies and procedures is to know your customers before executing any transaction. The main objective of Know Your Customer (KYC) is to determine identity and beneficial ownership of accounts, source of funds, the nature of customer's business and more. KYC process is mandatory and not a one-time process. It is on-going and continuous.

<u>Customers are grouped into two (2) categories:</u>

- ➢ Natural Persons (Individual Customer)
  - ✓ Resident
  - ✓ Non-Resident

➢ Legal Entities (Corporate Customers)

<u>Reference Screenshot – KYC Form</u>



30. CUSTOMER DUE DILIGENCE

Why Due diligence is necessary?

Money Laundering, Terrorist Financing, and Proliferation Financing is the process of concealing the proceeds of crime. One of the major steps in preventing ML/TF is the process establishing the true identity of the customer/supplier, to enable us to assess AML/CFT risk, associated with the customer or supplier. This process is called customer due diligence.

Crimes are always planned under covers and criminals pose the best and the most respectable persons, making it difficult for ordinary person to realize their true identities. Hence, The Company should be vigilant while dealing with both Walk in Customers & Regular Customers.

CDD (Customer Due Diligence) measures are processes that the Company requires to verify customer identities, understand the purpose of the relationship, monitor transactions, and keep customer information up to date to prevent financial crimes.

Customer due diligence is required whenever a customer wishes to conduct a transaction with the company. Due diligence is a continuous process & should be applied at different stages of a customer's relationship with the company.

It is the responsibility of all employees of the Company to apply due diligence while dealing with a customer.

Customer Due Diligence enables an organization to assess the extent to which its customer is exposed to a range of risks. By performing CDD, compliance department ensures to;

- Identify and verify counterparties/customers before establishing a business relationship, such as entering contractual commitments. This identified natural or legal person or authorized and fully identified agents should then be the only person or persons to whom payment is authorized to be made, or product delivered, unless legitimate and documented business reasons exist, and any third party is appropriately identified, and its identity verified;
- Identify beneficial owners and take reasonable measures to verify the identities, such that we are reasonably satisfied that we know who the beneficial owners are. The measures which must be taken to verify the identity of the beneficial owner will vary depending on the risk. For legal persons and arrangements this should include taking reasonable measures to understand the ownership and control structure of the counterparty/customer;
- Obtain information to understand the counterparty's/customer's circumstances and business, including the expected nature and level of proposed transactions;
- The details to be obtained have been specified in the attached Customer Registration form, both for Individuals and Legal Entities;
- For processing transactions, understand the customer's source of funds;
- For continuing overall business relationship, understand the customer's source of wealth; and
- During KYC renewing schedule, update KYC information for each client, retail and corporate.
- If the Company cannot reasonably identify and verify the ultimate beneficial owner, it will not start or will terminate the relationship and will consider filing an STR.
- Reference Screenshot – CDD Form

31. CUSTOMER DUE DILIGENCE - ON NATURAL PERSONS

Natural person who is holding valid ID's or entry permits which is approved by the United Arab Emirates and who wishes to register with the Company for availing services offered by the Company.
Natural Persons are categorized into two levels, such as; Resident and Non-Resident Customers.

Residents

Resident Customer refers to a person, who is either Citizen of United Arab Emirates or who has Resident Visa issued by the Government Authorities of UAE.

- Valid Emirates ID

Non-residents

Non-Resident refers to either Visit Visa holder which is issued by the Government Authorities of UAE or who have GCC National ID (Gulf Cooperation Council).

- Valid Passport with valid entry visa
- Valid GCC National ID (for GCC nationals)

Natural Person's onboarding Process:

- ✓ A new customer is being registered at the Company as per the UAE regulatory standards.
- ✓ Customer is allotted system generated Unique Identification Number (UIN) which is used for retrieval and tracking of transactions data of the particular customer. The UIN must not be assigned to more than one customer, and each customer must not be given more than one UIN.
- ✓ All identity documents must be physically checked and copied/scanned where required. The validity of the documents should be checked before acceptance.
- ✓ Staff shall register with the customer by entering/ capturing KYC information in LiveEx Shield AML - DNFBPs software from provided ID Documents.
- ✓ Prescribed IDs shall be obtained and scanned in LiveEx Shield AML - DNFBPs Software for feature inquiry / KYC purposes.
- ✓ ID should be valid. Expired ID is not acceptable. However, 30 days grace period has been given for the UAE resident customers of The Company.
- ✓ All the registered customers shall be risk rated with appropriate risk scores.
- ✓ If transaction appears to be carried out on behalf of another person/entity, vigilance is required i.e., it becomes necessary to identify that person/entity (the beneficial owner) as well as the representative bringing the transaction.

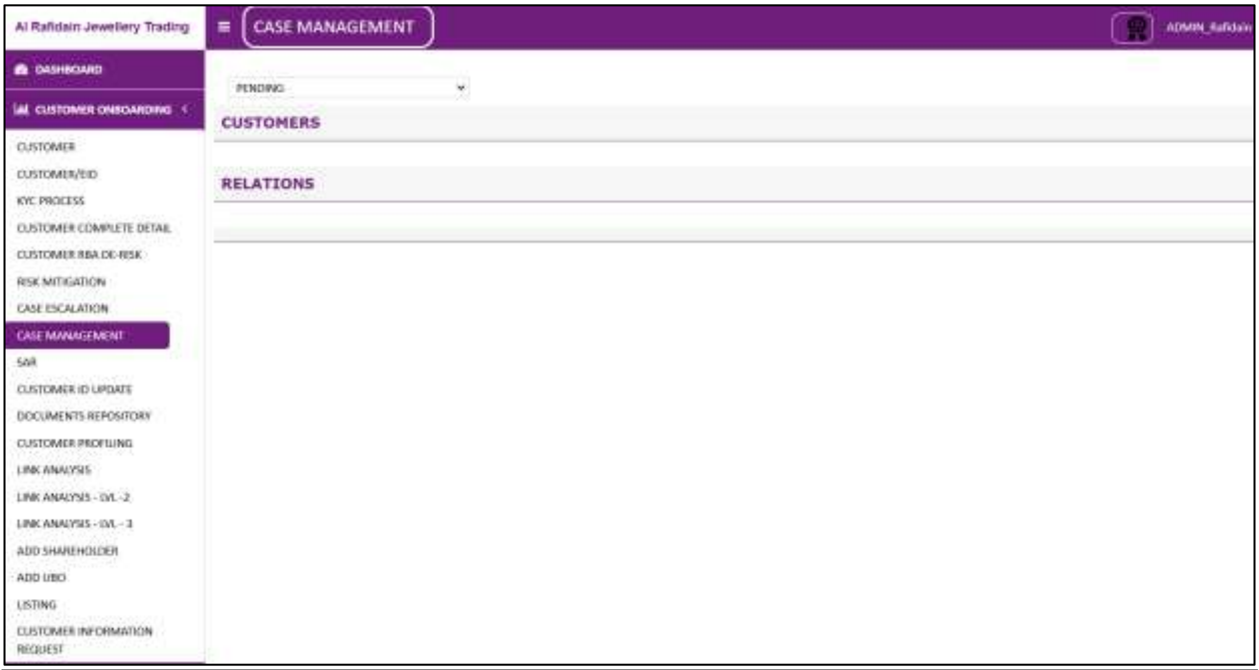
Compliance Approval

If the customer profile matched with any one of the following lists, the customer profile will be escalated to Compliance Approval an automatically;

- UAE Local Terrorist List
- UNSC Consolidated List
- Internal Watch List
- Dow Jones comprehensive list

The system will allow to carry any value of transaction upon the Compliance Officer approval only. For detailed guidelines please refer to the Section: - Sanction Screening

Reference Screenshot – Onboarding Compliance Approval



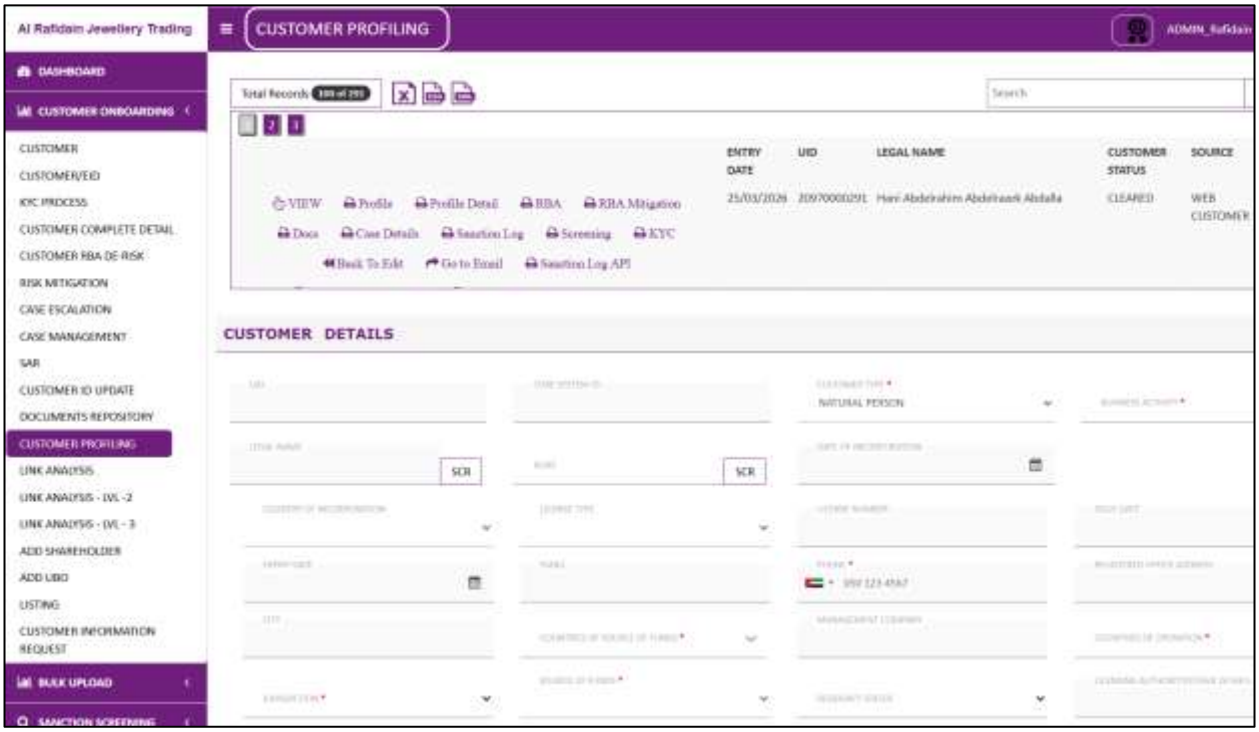
Updates, Changes & Modifications to Customer Profile

There may be significant changes in the customer's profiles and thus The Company must from time to time review and update the customer's profile. Natural Person's profile shall be reviewed and updated annually or whenever there are changes in the customer's information whichever comes first.

- Customer Name (if it is saved with wrong spells)
- Customer Nationality (if it is selected with wrong country)
- Customer Profession and Category (Salary leading to increased volume of transactions)
- Other significant changes may bring about a change in the pattern of transactions.

The updated customer's profile will require MLRO approval if any given parameters are matched with the sanction list or if the profile hits high risk score after changes are made.

<u>Reference Screenshot – Customer Profile Review</u>



The following components are available on the Compliance Officer menu for monitoring each customer profile.

- Customer Profile Simplified and Detailed
- Risk Based Approach
- Document Details
- Case Details – if any
- Sanction Screening Log
- KYC Form (CDD and EDD)
- Back to Edit - Checker control for customer profile edit
- Email Management

<u>Important Notes:</u>

- No transaction shall be undertaken before completion of the registration process, i.e., The Company shall carry out KYC on its customers in order to confirm who its customers are, and to ensure that the funds involved in the transaction originated from legitimate sources and used for legitimate purposes.

32. CDD REQUIREMENTS TO EXISTING CUSTOMERS

The Company applies CDD requirements to existing customers on the basis of materiality and risk. Due diligence on such existing relationships is conducted at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

- High-risk customers are subject to enhanced periodic reviews at least annually.
- Standard- and medium-risk customers are reviewed periodically, at intervals consistent with their risk profile.
- CDD measures must also be updated when there are material changes in a customer's profile, business activities, transaction patterns, or geographic exposure.
  All CDD updates and reviews are conducted in compliance with UAE AML/CFT

33. FAILURE TO SATISFACTORILY COMPLETE CDD

When the Company is unable to satisfactorily comply with relevant Customer Due Diligence (CDD) measures:

- The Company must refuse to commence the business relationship or perform the transaction; or
- Terminate any existing business relationship.

In all cases of refusal or termination:

- The matter must be documented, including the reasons for non-compliance with CDD.
- A Suspicious Activity Report (SAR) must be filed in the GOAML portal, as required by law.
- Records of the refusal, termination, and SAR filing must be retained in accordance with applicable UAE AML/CFT recordkeeping requirements.
- The case should be escalated to the Compliance Officer/MLRO for review and further action, where appropriate.

34. CDD AND TIPPING OFF

The Company, including its directors, officers, employees, and any third parties involved in customer transactions, are strictly prohibited from disclosing whether a Suspicious Transaction/Activity Report (STR/SAR), or any related information, is being reported to the GOAML Financial Intelligence Unit (FIU).

Violation of this prohibition ("tipping off") may constitute a criminal offence under UAE law and may lead to disciplinary or legal action.

35. ENHANCED DUE DILIGENCE

Enhanced due diligence (EDD) is to take additional measures, besides usual customer due diligence, to know more about the customer and his/her transactions to confirm that the transactions and funds are legitimate and free from any criminal link. EDD is conducted in accordance with Federal Decree-Law No. 10 of 2025, Cabinet Decision No. 74 of 2020, and applicable FATF standards.

Enhanced due diligence is not required in all circumstances; it is applied where the customer and the product/service combination are considered to be a greater risk and also in cases where there is doubt or suspicion with regard to the activities conducted by the customer. This higher level of due diligence is required to mitigate the increased risk. Examples of EDD measures include verifying the source of funds and wealth, obtaining additional identification documents, monitoring transactions more frequently, and conducting enhanced background checks.

36. EDD FOR NATURAL PERSONS (RESIDENT / NON-RESIDENT)

Customers' Enhanced Due Diligence (EDD) for natural persons shall be conducted in compliance with Federal Decree-Law No. 10 of 2025, Cabinet Decision No. 74 of 2020, and FATF Recommendations, based on the following scenarios:

- ➢ All high-risk customers who are natural persons, including PEPs and customers from high-risk jurisdictions.
- ➢ All high-risk transactions by natural persons.
- ➢ Name matches in sanction/watchlist screening.
- ➢ Suspicious transactions identified.

EDD procedures include:

- Verify and validate the customer's identity.
- Conduct transaction trend analysis.
- Obtain documentary evidence of the source of funds.
- Understand the customer's profile including occupation.
- Complete Risk Matrix and rate customer – High, Medium, or Low Risk.
- Identify suspicious transactions or customers.
- For PEPs, obtain approval from Senior Management and apply enhanced ongoing monitoring.

Source of funds and purpose of transactions must be verified, and supporting evidence (e.g., bank statements) collected, especially for cash transactions or where there is doubt. Receipts must be signed by the customer and retained along with all KYC/EDD documents for at least 5 years.

Special attention is given to visitors to the UAE; EDD is performed regardless of transaction value if there is any doubt or suspicion. Ongoing monitoring of high-risk customers is mandatory, and risk ratings should be updated whenever new relevant information arises.

37. ENHANCED DUE DILIGENCE FOR LEGAL ENTITY / CORPORATE CUSTOMER

- Legal Entity / Corporate Customers refers to any firm, establishment or company registered and incorporated at and under the laws of United Arab Emirates and who wishes to register with The Company for availing services offered by the Company.

- Relationship with a business entity such as a company should obtaining and verifying suitable documents in support of name, address and business activity – such as a copy of a business registration, a certificate of incorporation, a memorandum of articles of association, passport copies of the directors and shareholders, proof of address, or beneficial owner verification.

- Details of all employees who would be authorized to transact on behalf of the company, or firm and documents of their identification, together with their signatures – should also be requested. Copies of all documents called for verification should be kept on record.

- The controls built in the system ensure that customer and UBO information is mandatory to obtain while processing a transaction. This is a vital preventive approach that supports effectively filtering suspicious activity in a proactive manner, and in compliance with regulatory requirements.

LEGAL ENTITY / CORPORATE CUSTOMER ONBOARDING PROCESS

A. DOCUMENT COLLECTION PHASE (KYC):

- Legal Entity information (Company details, directors, beneficial owner, etc.)
- Identification records (trade license, ID proofs of UBO)
- Other required documents (MOA, AOA, certificate of Incorporation, audited financials, bank statements etc.)

Checklist for Legal Entities (Corporate Customers)

S.No.	Documents
1	Customer profile / KYC Form
2	Trade License Copy (Full set)
3	VAT Registration Certificate
4	Proof of Address -Latest Telephone/Electricity bill copy/Tenancy copy
5	Memorandum of Association / Power of Attorney / Article of Association

6	Partners – UAE National – Passport & Emirates Id Copy
7	Partners - Expatriate – Passport with valid visa, Emirates Id
8	Ultimate Beneficiary Details
9	Authorization Letter for Representative and ID copies with Mobile Number
10	Free Zone Company needs Lease Agreement/Tenancy Contract
11	Supply Chain Declaration

B. VERIFICATION

- Confirmation about the physical appearance (business address)
- Business Activities are aligned with Trade License or not
- Verifying Telephone Number and Email ID

C. APPROVAL

- Manager may accept or decline the case based on the Risk Level
- Case may revert to client to obtain more information or documents
- PEPs shall undergo compliance and Manager in charge approval

D. DATA INPUT

- The customer profile, i.e., the corporate customer documents and collected information are saved into LiveEx Shield AML - DNFBPs Software.
- Company System has detailed customer segregation function to identify the customer type, Nature of business with risk assessment.

E. SANCTION SCREENING

The Company Software will screen the customer and partner / UBO details. The profile will escalate to compliance approval if any matches against the sanction list (Dow Jones, UNSC, Local Lists, OFAC Consolidated and EU Consolidated List).

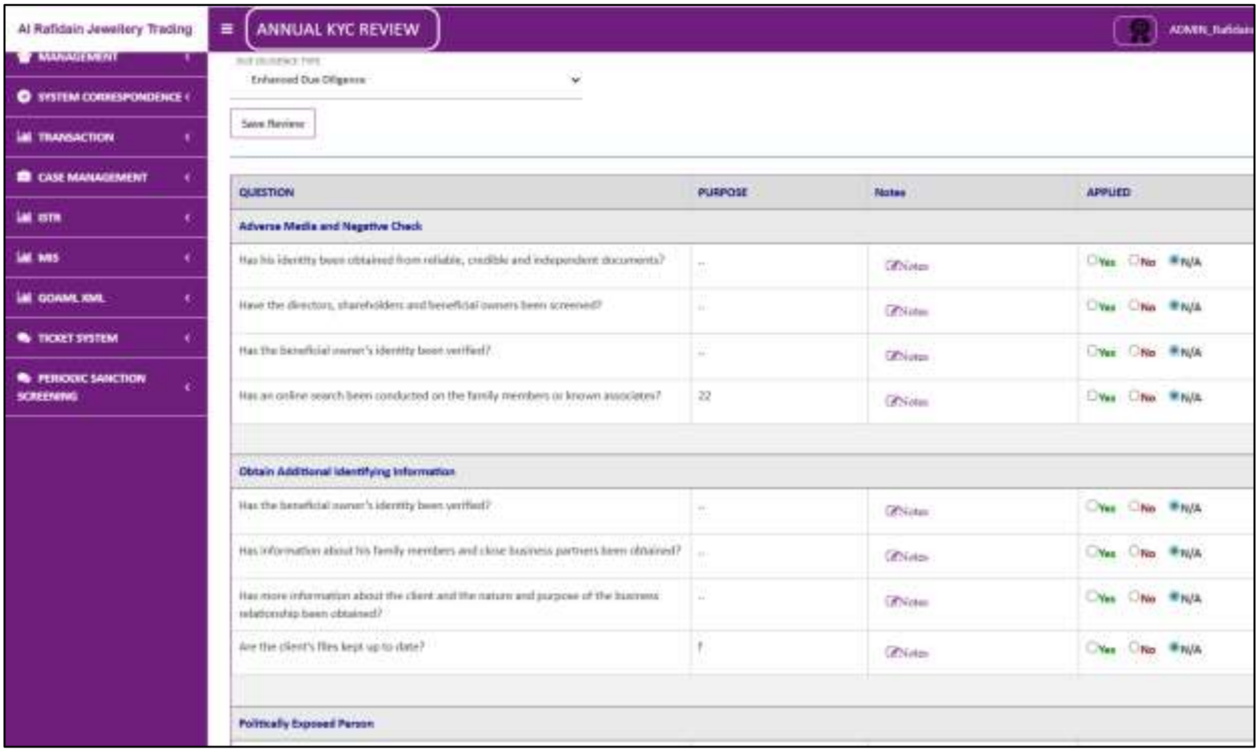
F. COMPLIANCE APPROVAL

If the customer profile or any one of the party matched with the following lists, the system will automatically escalate the profile to compliance officer approval.

- ✓ UAE Local Terrorist List
- ✓ UNSC Consolidated List
- ✓ Internal Watch List
- ✓ Dow Jones comprehensive list

The system will allow to carry any value of transaction upon the compliance officer approval only. For detailed guidelines please refer to the Section: - Sanction Screening

Reference Screenshot – EDD Form



38. EDD FOR HIGH-RISK CUSTOMER

Federal Decree-Law No. 10 of 2025 defines High-Risk Customers as including those who represent a risk:

"Either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a customer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party..."

High-Risk Classification:

The level of complexity and transparency of the customer's transactions, especially in comparison with the customer's or Beneficial Owner's educational and professional background.

The level of complexity and transparency of the customer's legal structure of legal persons or arrangements.

The nature of any other business interests of the customer or Beneficial Owner, including any other legal persons or arrangements owned or controlled.
Consistency between the customer's line of business and that of the counterpart to the customer's transactions (as identified, for example, through internet searches).
The Company is obliged to collect the following documents / additional information / evidence from high-risk customers such as:

- Source of wealth;
- Financial statements;
- Banking references;
- Description of the customer's primary trade area and whether international transactions are expected to be routine;
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and
- Explanations for changes in business activity.

39. REQUIREMENTS FOR HIGH-RISK COUNTRIES

The Company adopts Enhanced Due Diligence (EDD) measures that align with the Money Laundering (ML) and Financing of Terrorism (FT) risks related to Business Relationships and transactions involving customers from high-risk countries, which are subject to a Call for Action and Jurisdictions under Increased Monitoring, as well as the countries identified by NAMLCFTFC. Similarly, for legal persons and arrangements, the Company applies EDD to the Beneficial Owners, beneficiaries, and other controlling persons from high-risk countries.
The Company seeks guidance on high-risk countries from various sources, including NAMLCFTFC, the FATF list of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring, and NRA reports. Additionally, the Company refers to the Organization for Economic Cooperation and Development (OECD) list of jurisdictions classified as tax havens. The Basel AML index also serves as a valuable resource to assess the risk associated with a country.

Examples of some of the measures the Company applies to in this regard include:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to the identity of customers, Beneficial Owners, beneficiaries and other controlling persons;
- More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- Increased investigation to ascertain whether the customers or related persons (Beneficial Owners, beneficiaries and other controlling persons, in the case of legal persons and arrangements) are foreign PEPs;
- Increased supervision of the Business Relationship, including the requirement for higher levels of internal reporting and senior management approval, more frequent monitoring of transactions, and more frequent review/ updating of customer due diligence information.

Additionally, the Company implements all specific CDD measures and countermeasures regarding High-Risk Countries as defined by the National Committee for Combating Money

Laundering and the Financing of Terrorism and Illegal Organizations, including those related to the implementation of the decisions of the UN Security Council under Chapter VII of the Charter of the United Nations, the International Convention for the Suppression of the Financing of Terrorism and the Treaty on the Non-Proliferation of Nuclear Weapons, and other related directives, and those called for by the Financial Action Task Force (FATF) and/or other FSRBs.
In line with Federal Decree-Law No. 10 of 2025, the Company additionally ensures that enhanced due diligence measures for high-risk countries explicitly include identification, assessment, and mitigation of **Proliferation Financing (PF)** risks, and strict implementation of **Targeted Financial Sanctions (TFS)** as mandated under the new law.

40. EDD FOR POLITICALLY EXPOSED PERSON (PEP)

The AML-CFT Law and the AML-CFT Decision define PEPs as:

“Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organization or any prominent function within such an organization; and the definition also includes the following:

- Direct family members (of the PEP, who are spouses, children, spouses of children, parents).
- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP.
- Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

The Company implemented the real time sanction screening with API methodology from the “Dow Jones” service provider to identify the PEP and their associates. Also, the Compliance Officer / MLRO will conduct further screening from;

- Manual internet search protocols;
- Public or private databases;
- Publicly accessible or subscription information aggregation services;
- Commercially available background investigation services.

If a customer, Beneficial Owner, beneficiary, or controlling person is identified as a PEP, the compliance officer will take reasonable measures to establish the PEP’s source of funds and source of wealth and evaluate the legitimacy of the source of funds and source of wealth, including making reasonable investigations into the individual's professional and financial background.

Senior Management approval is mandatory before establishing a Business Relationship with a PEP, or before continuing an existing one. In regard to the latter, senior management should be notified, and their approval should be obtained for the continuance of a PEP relationship each time any of the following situations occur:

- An existing customer, Beneficial Owner, beneficiary, or controlling person becomes, or is newly identified as, a PEP;
- An existing PEP Business Relationship is reviewed and the CDD information is updated, either on a periodic or an interim basis, according to the organization's internal policies and procedures;
- A material transaction that appears unusual or illogical for the PEP Business Relationship is identified.

  Controls: PEP Approval form will be applied if the UBO identified as a FPEP or HIO.

  In line with Federal Decree-Law No. 10 of 2025, the Company also ensures that PEP relationships are assessed for Proliferation Financing (PF) risks, particularly where the PEP or related parties are connected to high-risk or sanctioned jurisdictions, and applies additional controls where required under the strengthened TFS obligations.

41. HIGH-RISK JURISDICTIONS

As per the FATF's High-Risk Jurisdictions subject to a Call for Action – 24 October 2025 update, the Company maintains strict protocols regarding dealings with countries identified as presenting significant ML/TF/PF risks.

In line with Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and the Financing of Illegal Organizations, and with reference to the competences of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations (NAMLCFTC), the Company adheres to all obligations applicable to DNFBPs concerning high-risk jurisdictions.

High-Risk (Black-List) Countries identified by FATF as of 13 February 2026 are:

- Democratic People's Republic of Korea (DPRK)
- Iran
- Myanmar

As per our internal policy, the Company will not engage in any business relationships or transactions with any individuals or entities operating within the above jurisdictions. We are committed to upholding the integrity of our operations and safeguarding ML/TF/PF risks associated with such dealings.

If we become aware that any of our suppliers or customers are engaged in activities connected to these jurisdictions, the Company will:

• Immediately terminate the business relationship and block any further transactions;
• File an STR/SAR with the UAE Financial Intelligence Unit (FIU) via the goAML portal where applicable;
• Notify the relevant competent authorities, ensuring all required regulatory steps are taken.

The Company remains fully committed to maintaining compliance with all applicable AML/CFT/CPF legislation and international standards. These measures are essential for protecting our operations and ensuring the trust and confidence of our stakeholders.

The Company will also continuously monitor FATF publications and UAE competent authority circulars to ensure the High-Risk Jurisdictions list is kept updated at all times.

42. JURISDICTIONS UNDER INCREASED MONITORING

As per the Financial Action Task Force (FATF) “Jurisdictions Under Increased Monitoring” list (grey-list) — see full list published on the FATF website — the Company is committed to adhering to the highest standards of compliance, particularly concerning the identification and mitigation of risks associated with jurisdictions on this list.

In line with Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and the Financing of Illegal Organizations, and with reference to the competences of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations (NAMLCFTC), and the relevant implementing regulations, the Company ensures strict compliance regarding dealings with jurisdictions under increased monitoring.

FATF Grey-List Countries (as per FATF website list)

The jurisdictions currently listed under Increased Monitoring by FATF include (subject to periodic updates):

Jurisdictions under Increased Monitoring – 13 February 2026

Country
Algeria, Angola, Bolivia, Bulgaria, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Haiti, Kenya, Lao PDR, Lebanon, Monaco, Namibia, Nepal, South Sudan, Syria, Venezuela, Vietnam, Virgin Islands (UK), Yemen, Kuwait, Papua New Guinea

High-Risk Jurisdictions subject to a Call for Action - 13 February 2026

Democratic Republic of Korea
Iran
Myanmar

Source: FATF — Black and Grey Lists web page.

(https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html)

Risk-Based Compliance Measures

To ensure robust compliance, the Company applies a comprehensive risk-based approach when interacting with customers or transactions involving these jurisdictions, including:

- Full customer and beneficial-owner identity verification and documentation for natural and legal persons.
- Ongoing monitoring and periodic reviews of customer due diligence information.
- Enhanced Due Diligence (EDD) for customers, beneficial owners, controlling persons, or transactions linked to grey-listed jurisdictions.
- Additional scrutiny, including obtaining reliable independent evidence for source of funds / wealth, nature of business, transaction purpose, and business counterparties.
- Senior management approval for new or continued business relationships involving high-risk jurisdictions.
- Documentation of rationale for acceptance or rejection of business relationships, and enhanced monitoring where accepted.

By consistently applying these measures, the Company maintains a strong compliance culture and mitigates ML/TF/PF risks arising from transactions with or involving jurisdictions under increased monitoring.

43. APPROVAL AND ESCALATION LEVELS

Customer Type	Activity	Value	Preventive Measure Required
Natural Persons	Any Activity	AED 1 - AED 55,000/-	CDD
Natural Persons	Any Activity	AED 55,000/- and above	EDD
All Legal Persons or Arrangements	Any Activity	Any Value	EDD

PEPs	Any Activity	Any Value	EDD
DNFBPS and other DPMS	Any Activity	Any Value	EDD
High-Risk Natural Persons	Any Activity	Any Value	EDD
High-Risk circumstances	Any Activity	Any Value	EDD

44. CASH ACCEPTANCE AND REPORTING MEASURES

44.1 PROCEDURES OF CASH TRANSACTIONS

Before conducting the cash transactions and as per our internal policy below EDD measures to be completed:

1. Customer Identification and KYC (EDD Measures)
    - Customer Identification and KYC details must be entered into and completed in AML system (Customer registration)
2. Collect and complete the INDIVIDUAL CUSTOMER CDD/EDD FORM (format Given Below)
3. Collect supporting documents such as ID copies, source of fund documents, CDF forms (Customs Declaration Form-cash declaration 60,000 AED above)

44.2 REPORTING MEASURE

As per Federal Decree-Law No. 10 of 2025 and Circular No 08/AML/2021 dated 02 June 2021, transactions with entities /companies, the Company ensures compliance with cash reporting measures by verifying and documenting all cash transactions equal to or exceeding AED 55,000. These DPMSR transactions are reported to the FIU via the GoAML portal. Records are securely maintained for five years, with suspicious activities promptly escalated.

45. SANCTIONS AND PEPs SCREENING

The Company, software is configured to execute a real – time name screening on every customer, beneficiary / beneficial owner / partner's /shareholders, representatives, and all parties involved in the transaction activity. Every customer onboarding and Transaction will be screened related to blacklisted or sanctioned entities. Therefore, when a generated alert is investigated, the Compliance Officer / MLRO considers the following variables in order to identify possible matches:

a) Full Name

b) Nationality

c) Date of Birth

d) Place of Birth

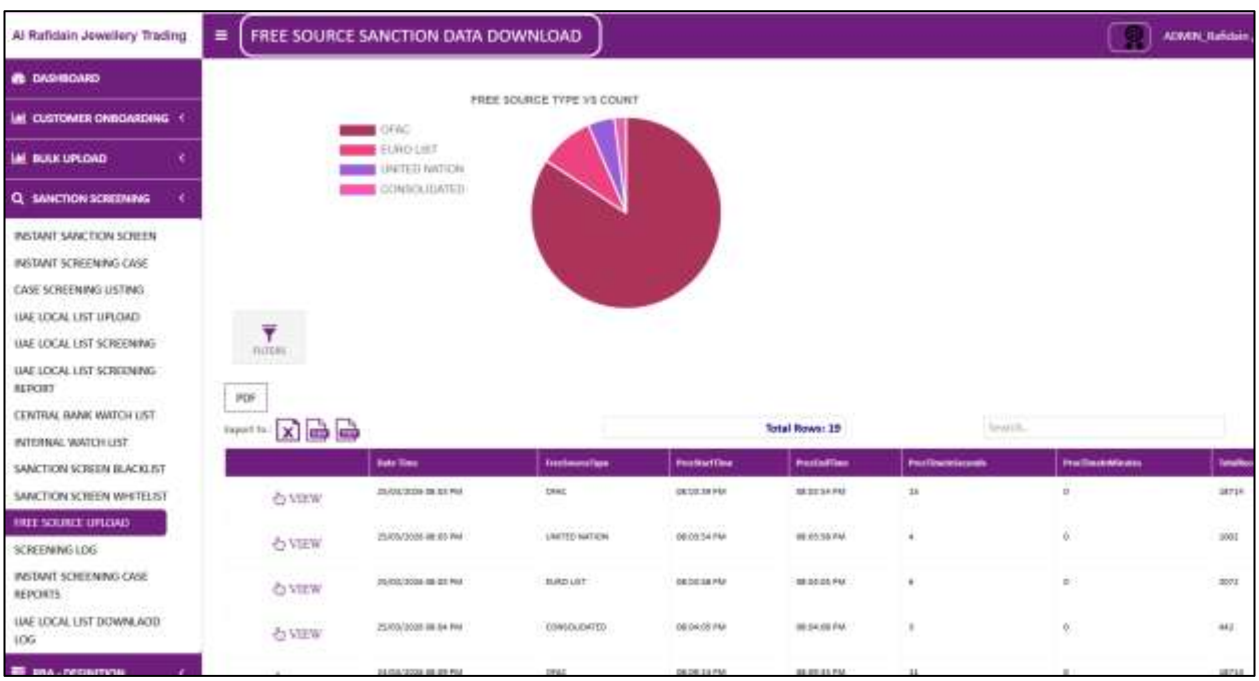
Sanctions screening refers to the process of screening customer details against the different lists of sanctions for PEP status and whether the customer is involved in money laundering or terrorist activities. The customer details are screened in the following list:

- ✓ UNSC: United Nations Security Council Consolidated List;
- ✓ UAE - Local Terrorist List
- ✓ OFAC: Office of Foreign Assets Control - Specially Designated Nationals List (SDN)
- ✓ OFAC: Office of Foreign Assets Control - Consolidated Sanctions List;
- ✓ EU: European Union Consolidated list;
- ✓ Dow Jones; and
- ✓ Internal Watch List.

Company makes use of LiveEx Shield to screen customers against recognized Sanctions Lists and Politically Exposed Persons (PEPs) lists.

Company will take all required steps to ensure that all customers with whom a business relationship is established are screened against relevant notices.
We are conducting EDD on all PEPs / FPEPs / HIOs / PEP Associates / Diplomatic Passport Holders, whether natural person customers or the UBOs of legal persons or legal arrangements. Before establishing a relationship with the customer, we obtain senior management approval and continue an existing one, ensure that the customer undergoes review checks and verification at least on an annual basis or prior to carrying out the first transaction following the expiration of the 12-month period.

<u>Reference Screenshot – Screening Sources</u>



46. TRANSACTION MONITORING

A well- defined transaction monitoring program is an important component of an effective AML & CFT program. As a financial services industry the Company has come under immense regulatory pressure to improve and expand monitoring and surveillance of transactions for the purpose of preventing and detecting money laundering & financing of terrorism activities.
The primary objective of the Company is to concentrate on actual risks, customer and product clarification and to reduce the number of chances of company from being misused.
Basic Rules for Transaction Monitoring:

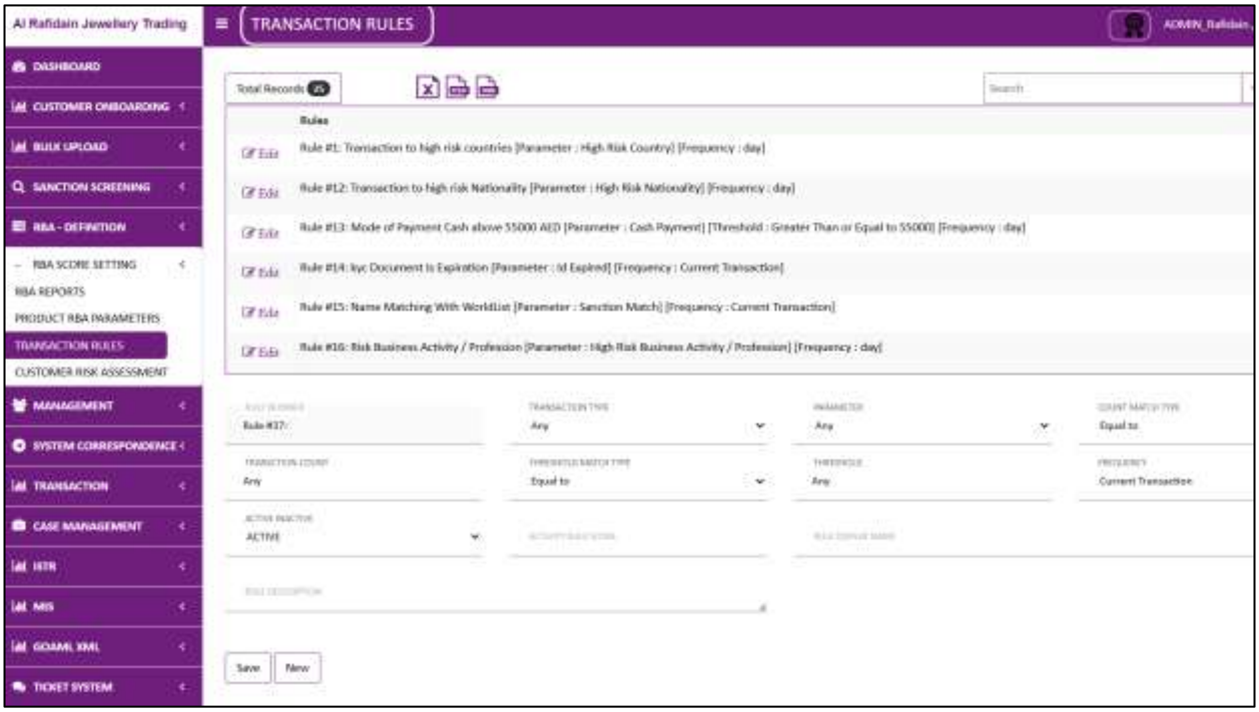
The 5 "W" s are:

a) *Who - is the customer- individual or corporate, what is the profile of the customer?*
b) *What - product is the customer availing, Gold, Diamond or any other product?*
c) *Where - is the customer remitting funds to? Is the country a high-risk jurisdiction? Is there a valid reason for remitting funds?*
d) *Why - is the customer remitting funds? Does the transaction make economic sense and what is the exact purpose?*
e) *Whom – for whom is the transaction being conducted, who will benefit from the transaction? Who is the Ultimate beneficiary?*

The Company adopts a risk-based approach to transaction monitoring, which includes 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.
- Concern officer will review customer records to ensure that documents, data and information collected during the KYC, CDD and monitoring processes are relevant and up to date.
- The Compliance officer investigates any unusual or suspicious transactions and maintains all supporting records for a minimum period of 5 years.
- Following the investigation of unusual transactions, if there are reasonable grounds for suspicion, our Compliance Officer will immediately report such transactions to FIU.

Transaction Monitoring Rules



47. RED FLAG INDICATORS

A suspicious transaction includes any activity which does not fit with the normal course of business. Few indicators as per Federal Decree law can be noted as below:

- Splitting of transactions
- New / walk in customer carrying large transaction
- New / Walk in customers seeks to buy high value of gold, diamond and precious metals
- Customer is not cooperating in answering questions and refuses to give supporting documents pertaining to his transactions
- Customer who cannot provide ID when requested with the obvious intention to hide his identity
- Customers who cannot justify the source of funds
- Politically exposed person, their family and staff
- Cash brought in from countries with a high level of corruption or political instability
- Unusual pattern and volume of the customer transaction
- Transaction is not in line with the customer's business activity listed in their trade license

- Pattern of transactions has changed since business relationship was established.

Proliferation Financing (PF) Red Flags

- Payments or routing inconsistent with legitimate PMS trade patterns or involving PF high-risk jurisdictions (e.g., FATF grey/blacklists).
- Customers requesting dual-use commodities, evading export controls, or dealing in goods subject to Federal Decree-Law No. 43 of 2021.
- Matches against EOCN/PF-related TFS lists (beyond standard terrorism sanctions) or unusual supply chain actors (miners/refiners from high-risk origins).
- Complex corporate structures, front companies, or procurement patterns inconsistent with stated DPMS business (e.g., gold imports from countries without known mines).

48. SUSPICIOUS TRANSACTION AND SUSPICIOUS ACTIVY REPORT (STR and SAR)

STRs shall be filed without delay upon suspicion or reasonable grounds to suspect ML/TF/PF, including attempted transactions, historical activity, or partial proceeds regardless of value, as required under Federal Decree-Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025. Reporting does not require certainty of criminality.

For the purposes of this Policy and in accordance with Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing, and its implementing Cabinet Resolution No. 134 of 2025, a suspicious transaction refers to any transaction, attempted transaction, or funds which the Company has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or timing—any of the following:

The proceeds of crime (whether designated as a misdemeanor or felony, and whether committed within the UAE or in another country where it is also a crime).

Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organizations.

Being intended to be used in an activity related to such crimes.

It should be noted that the only requirement for a transaction to be considered suspicious is "reasonable grounds" in relation to the conditions referenced above. The suspicious nature of a transaction can be inferred from certain information, including customer due diligence information, transaction behavior, and risk indicators, and it is not dependent on obtaining evidence that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved.

Transactions need not be in progress or pending completion to be considered suspicious. Even past transactions, regardless of timing or completion status, which are found upon review to give reasonable grounds for suspicion, must be reported.

All suspicious transactions must be promptly reported to the MLRO, who will evaluate and submit the STR to the FIU via the goAML system without delay as soon as suspicion or reasonable grounds for suspicion arise, regardless of the transaction amount or whether the transaction is completed.

The Company shall maintain records of all STRs, related documentation, and MLRO assessments for a minimum of five (5 to 10) years, ensuring they are retrievable for regulatory review or internal audit.

Internal Escalation Flow for STR/SAR:

1. Employees identify unusual or suspicious activity based on this Policy, red flag indicators, and their knowledge of the customer.
2. Employees immediately stop any further processing of the transaction (where feasible) and escalate all details and documents to the MLRO using the internal incident/escalation form.
3. The MLRO assesses suspicion, documents the rationale, and, where reasonable grounds for suspicion exist, files an STR/SAR through the goAML system without delay, and applies any required risk-mitigation measures.
4. The MLRO maintains records of all escalations, assessments, and submitted or declined STRs/SARs for at least five (5) years in line with the record-keeping requirements of this Policy.

49. SUSPICIOUS ACTIVITY INDICATORS

The Company will furnish a list of Suspicious Activity Indicators for its employees.
The existence of Suspicious Activity Indicators does not necessarily imply criminality but serves as a trigger for Enhanced Due Diligence (EDD), further investigation, and assessment by the Compliance Officer.
These indicators are part of the Company's risk-based approach to AML/CFT and may lead to reporting of suspicious activity to the MLRO for evaluation and potential submission to the Financial Intelligence Unit (FIU) via the GoAML system.

50. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

When identifying suspicious transactions, the Company and its management and employees should be aware that, in relation to ML/FT crimes, there is no minimum threshold or monetary value for reporting, and no amount or transaction size should be considered too small for suspicion. This is particularly significant for financing of terrorism and illegal organizations, as typologies related to these may often involve very small amounts of money.

All transactions that raise suspicion must be promptly reported to MLRO, who will assess and submit the STR if required.

The following are examples of potentially suspicious transaction types (illustrative and not exhaustive):

- Transactions or series of transactions that appear unnecessarily complex, that make it difficult to identify the customer or Beneficial Owner, or that lack a discernible economic rationale.
- Numbers, sizes, or types of transactions that appear inconsistent with the customer's expected activity or previous activity.

- Transactions appear significantly larger than the customer's declared income or turnover.
- Transactions involving high-risk countries, including "own funds" transfers, especially where there is no clear reason for the specific transaction routing.
- Situations in which CDD measures cannot be completed, such as when customers or Beneficial Owners refuse to provide required documentation, or provide documents that are false, misleading, fraudulent, or forged.
- Employees should consider risk factors in combination and exercise professional judgment when identifying potentially suspicious activity.
- STRs must explicitly identify potential PF alongside ML/TF risks per Section 15 indicators, using goAML PF-specific reporting fields (Proliferation Financing typology) and referencing EOCN/TFS matches where applicable.

51. TIMING OF SUSPICOUS TRANSACTION REPORT

Employees must immediately report any suspicious transaction internally to MLRO. The MLRO and Compliance Department are then responsible for submitting the verified STR to the GoAML – FIU portal **without any delay**, regardless of whether the transaction has already been completed.

52. SUSPICIOUS TRANSACTIONS REPORTING USING GOAML SYSTEM

The Company follows the GoAML portal for all STR and SAR submissions, in line with UAE AML/CFT obligations.
Employees must report any suspicious transactions internally to the MLRO, who is responsible for submitting verified STRs via GoAML.
The GoAML application is a fully integrated software solution developed for use by Financial Intelligence Units (FIUs) and is one of UNODC's (United Nations Office on Drugs and Crime) strategic responses to financial crime, including money laundering and terrorist financing. FIUs play a leading role in any anti-money laundering regime, as they are generally responsible for receiving, processing, and analyzing reports made by entities in accordance with UAE regulations.
GoAML is specifically designed to meet the data collection, management, analytical, document management, workflow, and statistical needs of Financial Intelligence Units.

53. TIPPING OFF

- In accordance with UAE AML/CFT requirements, all suspicious transactions must be kept fully confidential, and no employee, manager, or representative shall inform any customer or third party that a transaction is being reported or investigated.
- Non-compliance with this prohibition may result in immediate termination, and the individual may be personally liable for fines, imprisonment, or both.
- Staff, senior management, and representatives of the Company are strictly prohibited from directly or indirectly disclosing that a transaction is under review, being monitored, or reported to the FIU. Such actions constitute "Tipping-Off", which is a criminal offence.

- The Compliance Department ensures, through ongoing training and detailed procedures, that all employees are aware of the consequences of tipping-off. All staff receive adequate AML/CFT training to prevent tipping-off incidents.
- Any person who violates this prohibition is liable to a penalty of not less than AED 100,000 and not more than AED 500,000, and imprisonment for a term of at least six months, as prescribed under UAE law.

54. PROTECTION AGAINST LIABILITY FOR REPORTING PERSONS

The Company as well as their Owner members, employees and authorized representatives, are protected by the relevant articles of the AML-CFT Law and AML-CFT Decision from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This is also the case even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. However, it should be noted that such protections do not extend to the unlawful disclosure of the customer or any other person, whether directly or indirectly, that they have reported or intended to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

55. HANDLING OF BUSINESS RELATIONSHIPS AFTER FILING OF STR'S

Once a Suspicious Transaction or other suspicious information related to a customer or business relationship has been reported to the FIU:
The MLRO/Compliance Department is obliged to follow any instructions from the FIU or competent authorities regarding the specific transaction and the overall business relationship.
The Customer or Business Relationship should be classified as High-Risk, and appropriate risk-based Enhanced Due Diligence (EDD) and ongoing monitoring must be applied.
In the case of a confirmed STR, the business relationship with the given customer or entity should be documented and marked as High-Risk by the Compliance Department. All future transactions must be conducted under risk-based EDD with approval from the Compliance Department, and ongoing due diligence must be performed and properly documented.

56. EXTERNAL COMPLIANCE ENQUIRIES

The MLRO/Compliance Department is responsible for responding to and handling external compliance enquiries as follows:

- Respond promptly and in accordance with regulatory timelines to any reasonable request for information from the AML Unit, Financial Intelligence Unit (FIU), or other competent authorities.
- Respond to banks, correspondent banks, and other financial institutions regarding AML questionnaires and related documents.

Ensure that all responses and supporting documentation are properly recorded and retained for audit and regulatory review purposes.

57. RECORD KEEPING

The Company, through the MLRO/Compliance Department, is obliged to maintain detailed records, documents, data, and statistics for all transactions, all information obtained through CDD/EDD measures, account files, business correspondence, and the results of any analysis undertaken. Records should also cover documents associated with ML/FT risk assessments and mitigation measures.

The objective of record keeping is to ensure that the Company can reconstruct transactions at the request of relevant authorities and provide supporting information for audits or regulatory inspections.

All records, including Customer IDs, Trade Licenses, Invoice details, EDD documents, account opening documents, customer profiles, STR/SAR reports, and screening logs, must be easily retrievable.

The Company will retain the following records for a minimum of five (5) years from the date of transaction or the end of the business relationship, whichever is later:

A. All CDD/EDD records.

B. Records of all AML/CFT training delivered.

C. Details of actions taken regarding internal and external suspicious activity reports.

D. Details of information considered by the MLRO/Compliance Department for internal reports where no external report was made.

E. Screening logs.

58. ONGOING MONITORING OF BUSINESS RELATIONSHIPS

The Company ensures that all documents, data, and information collected under the CDD process are kept up-to-date and relevant through periodic reviews of existing records, with particular focus on higher-risk customers or business relationships.

Ongoing customer due diligence (CDD) is the process of continuously monitoring and assessing customer relationships to ensure compliance with regulatory requirements and to mitigate risks related to money laundering, terrorism financing, fraud, and other financial crimes. This process includes:

Regular Monitoring: Continuously reviewing transactions and customer activities to identify unusual or suspicious patterns.

Updating Information: Periodically updating customer information, including identification details, ownership structure, and other relevant data, to reflect changes in the customer's risk profile.

Risk Assessment: Evaluating the risk level of each customer based on behavior, transaction patterns, geographic jurisdictions, and other relevant risk factors.

Enhanced Due Diligence (EDD): Applying more rigorous measures for high-risk customers, such as additional documentation, verification of beneficial ownership, or closer scrutiny of transactions.

Training and Awareness: Ensuring staff are trained to recognize red flags, understand emerging risks, and apply ongoing CDD effectively.

Reporting: Promptly reporting suspicious activities to the MLRO and relevant authorities in accordance with regulatory obligations.

Ongoing CDD is crucial for maintaining the integrity of the Company's operations and ensuring that it does not inadvertently facilitate illicit activities.

59. NO RETALIATION POLICY

It is the Company's strict policy that no employee, manager, or representative shall face any form of retaliation or prejudice for disclosing, in good faith, any information regarding money laundering or suspicious activity to the MLRO, Compliance Department, regulatory authorities, government agencies, or any other relevant body involved in the prevention of money laundering.

60. ANTI-BRIBERY POLICY

The Company strictly prohibits any form of bribery and corruption within the company, as well as with its business partners, service providers, customers as well as governmental agencies.

The Company takes a zero-tolerance approach to bribery and corruption, and we are very committed to acting professionally, fairly and with integrity in all our business dealings and relationships. It is our best practice objective that those we do business will take a similar zero-tolerance approach to bribery and corruption.

61. EXIT POLICY AND PROCEDURE

This policy and related procedures provide a clear exit process ensuring that clients are well informed, supported and smoothly transitioned from The Company.

Voluntary Client Exit

- Client no longer wishes to avail services provided by The Company.

Involuntary Client Exit

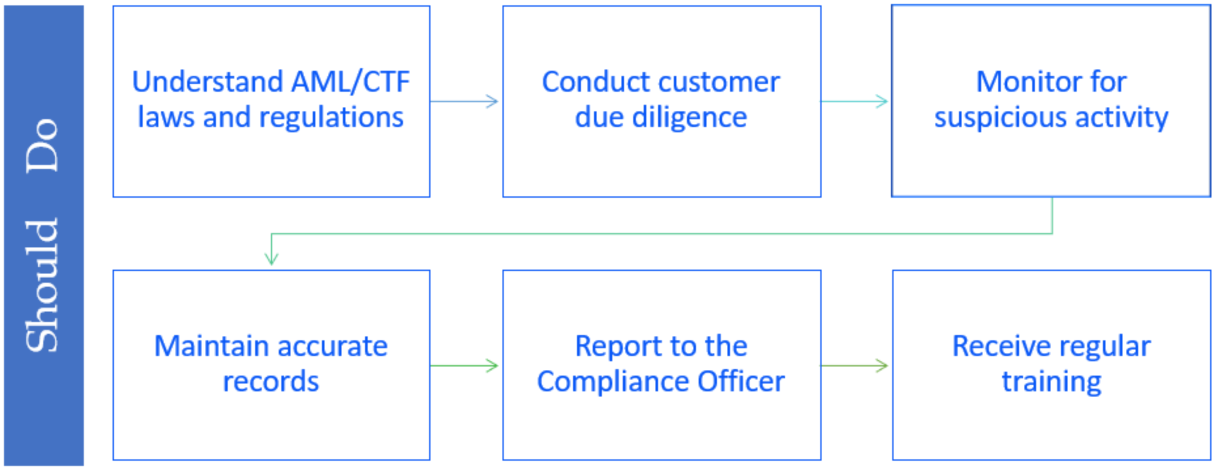
- When any suspicious activity is identified.
- When client enters sanctions list, it is blacklisted or involved in negative media news.
- When client is indulged in illegal activities
- If the client is reluctant to provide complete KYC or other supporting documents.
- If the client provided any manipulated, fake documents etc.
- If the Corporate Client has not executed transactions within 6 months interval from the date of account opening or date of last transaction with The Company.

62. KNOW YOUR EMPLOYEE

As a part of Know Your Employee (KYE) process, The Company do screen the candidate's name against sanctions and PEP lists before we issue the offer letter. Following information should be obtained by the company before hiring any new employee: -

- Identity Check / Passport Check
- Criminal Check (Good Conduct Certificate from Police of UAE/countries where the employee will be joining, for the last 5 years)
- Credit Check & Civil Litigation Check: Al Etihad Credit Bureau in UAE and other similar agencies in countries where the candidate is joining from.
- Education Qualification Check: We only take the attested document of their educational qualification. In case the job does not require educational qualification, we waive this clause off.
- Reference Check: We perform a reference check on the employee's previous employers.

63. EMPLOYEE RESPONSIBILITIES



- Always be vigilant – report knowledge or suspicion of Money Laundering.
- Know Your Customer (KYC)
- Establish true owner of funds
- Proper completion and approval of forms.
- Question legitimacy when in doubt.
- Report potentially suspicious or unusual transactions and activities
- Data input.
- Follow all internal circulars and instructions.
- Adhere to our Anti-Money Laundering policy and procedures.
- Be accountable for your actions & know your obligation – Ignorance is not an excuse.
- Not to knowingly assist in the laundering of criminal funds.
- Not to alert a suspected launderer.

64. STAFF TRAINING AND AWARENESS

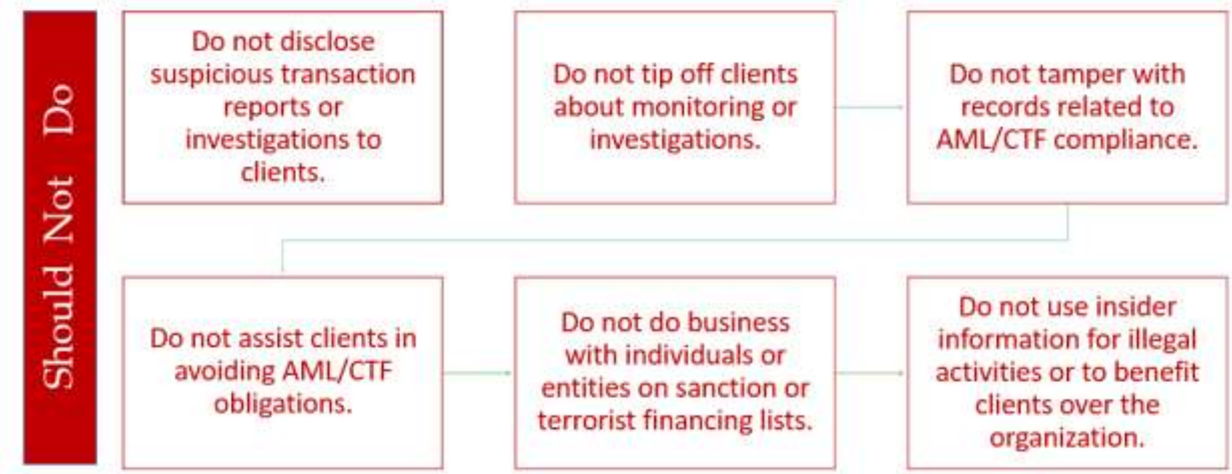
Staff and Senior Management shall receive periodic AML/CFT/CPF training covering emerging risks, including PF and virtual assets, consistent with Federal Decree-Law No. 10 of 2025. Training records must be maintained and reviewed annually.

The Company offers career building and skill enhancement measures through periodic in-house and outsourced training programs as well as offering the opportunity of participation in programs conducted by regulatory and professional bodies.

In order to maintain an effective AML & CTF program, it is imperative that all our employees understand this policy and are trained to identify and report suspicious activity. To achieve this goal, the Compliance Officer or a third party provides annual AML training to all relevant employees.

The Company segregated the Training and Awareness based on the followings;

- Training for New Employees
- On-Going Training Sessions (For Exist Employees and Senior Management)
- Continuous Professional Development (for Compliance Department)



- In order to maintain an effective AML & CTF program, it is imperative that all our employees understand this policy and are trained to identify and report suspicious activity. To achieve this goal, the CO or a third party provides annual AML training to all relevant employees.
- Comprehensive training must be provided to all employees including their manager in charge, functional heads and owners/partners/shareholders.
- The periodic training of all employees covers this policy, the KYC procedures, UAE and global regulations, particularly the identification and reporting of suspicious transactions.

- It is the policy of the Company to provide AML training to all relevant employees within 30 days of joining the company. Relevant employees include employees with customer contact, operational staff as well as senior management.
- Refresher Training must be provided to all employees at regular intervals to remain updated with any changes in provisions, regulations and AML/CFT law.
- Objective and content of the AML Training program will be responsibility of the CO.
- The Company ensures that the Compliance Officer and other employees of the AML/CFT Compliance Department must attend external training in AML/CFT compliance every year.

The Company - training will include, at a minimum:

- Money laundering and terrorist financing, definitions, typologies as well as recent trends.
- AML/CFT policies and procedures include the highlights of recent changes.
- The regulatory responsibilities and obligations of employees under AML/CFT Laws, Regulations, Notices and the Standards.
- Description of Know Your Customer (KYC).
- Due Diligence measures and procedure for monitoring transactions.
- Sanction screening and PEP screening procedures.
- Red flags to identify unusual transactions or transaction patterns or customer behavior.
- Processes and procedures of making internal disclosures of unusual transactions.
- Roles of the Compliance Officer / MLRO and Alternate Compliance Officer / DMLRO including their full contact details.
- Tipping off.
- Record retention policy.
- Reference to industry guidance and other sources of information.
- Penalties for non-compliance with the AML/CFT Laws, Regulations, Notices and the Standards.
- Disciplinary procedures to be applied to employees for not adhering to the AML Policy and Procedures.
- Any Updating and Regulations from the Regulator and the relevant Government Authorities.

What Is More Important Business or Staff or Compliance?

- All are equally important.
- All must be taken care of, always.
- The Company need Customers, NOT Money Launderers & Terrorist Financier.
- Maintain Excellent Customer Service while you practice Anti-Money Laundering Procedures.

65. INDEPENDENT INTERNAL AUDIT

The testing of our AML/CFT program will be performed at least annually (on a calendar year basis) by an independent third party. The Company will evaluate the qualifications of the independent third party to ensure they have a working knowledge of UAE AML/CFT law, FDL No. 10 of 2025, and its implementing regulations. Independent testing may be performed more frequently based on risk factors, regulatory changes, or audit findings.
The MLRO/Compliance Department, Manager, and other responsible personnel are responsible for coordinating the audit, ensuring that all findings and open audit points are addressed, and reporting progress to the Owner in a timely manner.
As per the guidelines, the independent audit will cover the following:

- Internal Audit Charter, Scope, and Methodology of the audit.
- Adequacy of AML/CFT and CDD policies, procedures, and processes, and whether they comply with regulatory requirements and FDL 10/2025.
- Assessment of the effectiveness of risk-based procedures, including identification and monitoring of high-risk customers, products, services, and jurisdictions.
- Assessment of training adequacy, including comprehensiveness, accuracy of materials, training schedule, attendance tracking, and escalation procedures for non-attendance.
- Review of outsourced AML/CFT compliance functions, including qualifications of personnel, contracts, performance, and reputation of the service provider.
- Review of case management and STR/SAR systems, including evaluation of research, investigation, and referral of unusual or suspicious transactions from all business lines.
- Review of record retention and reporting compliance, including STR/SAR filing, transaction monitoring, and documentation.
- Submission of the audit report with recommendations to the Owner, Manager, and Compliance Officer.
- Monitoring and tracking of remediation actions to ensure all recommendations are implemented in a timely manner.

66. VIOLATIONS AND ADMINISTRATIVE FINES

The Company acknowledges that any failure to comply with the requirements of Federal Decree-Law No. 10 of 2025 on Combating Money Laundering, Terrorist Financing and Proliferation Financing, its Executive Regulations (Cabinet Resolution No. 134 of 2025), and the applicable Cabinet Resolutions, including Cabinet Resolution No. 71 of 2024 concerning Administrative Fines, may expose the Company to administrative, regulatory, and criminal sanctions. Such sanctions may be imposed by the Ministry of Economy, other competent supervisory authorities, and/or the competent courts, and may include, without limitation, monetary fines, corrective and remedial measures, restrictions on business activities, suspension or cancellation of licences, and, where applicable, personal liability of directors, managers, and senior officers in cases of knowledge, consent, negligence, or failure to exercise due oversight.

Corporate Criminal Liability (Federal Decree-Law No. 10 of 2025)
Without prejudice to administrative penalties, violations of the Federal Decree-Law may result in criminal liability, including:

- Corporate fines of up to AED 100,000,000.
- Value-based fines of up to twice the value of the criminal property, where such value exceeds the maximum prescribed fine;
- Additional judicial measures, including dissolution of the legal entity and closure of business premises; and
- Personal criminal liability for directors, managers, or officers where offences are committed with their knowledge, consent, or as a result of negligence or failure to exercise appropriate supervision.

Administrative Fines
The unified list of administrative violations and corresponding fines applicable to Designated Non-Financial Businesses and Professions (DNFBPs) is set out in Cabinet Resolution No. 71 of 2024, which is incorporated by reference into this Policy and shall apply as issued and amended from time to time.

Official source:
https://uaelegislation.gov.ae/en/legislations/2546/regulations

67. DISCIPLINARY ACTIONS

Disciplinary actions to Employees in case of violation / breach of the Policies and procedures
The employees of the Company will receive disciplinary action from the Senior Management not limited to verbal warnings, warning letters, dismissal and termination depending on the severity of the action done by the employee not adhering to the Policy and Procedures.
Company is committed to following strict compliance with the law and a corporate culture that values and promotes honesty and integrity in operations. The Company has taken measures to detect and prevent fraud, abuse, and other non-complaints practices. The Compliance Program's Disciplinary Policy applies to all employees including executives, functional heads and managers who are active participants.
Stage 1 – Improvement Note: Unsatisfactory Performance
Stage 2 – First Warning: Failure to Comply
Stage 3 – Dismissal

68. SENIOR MANAGEMENT APPROVAL

Senior management has approved this AML/CFT compliance program in writing as reasonably designed to achieve and monitor our Company's ongoing compliance with the requirements of the AML/CFT law and the implementing regulations under it. This approval is indicated by signatures below.

69. INTERNATIONAL FINANCIAL SANCTIONS

The UAE is a member of several multinational and international organizations and governing bodies, including the United Nations. As such, the UAE is a party to many international agreements and conventions pertaining to the combating of money laundering and the financing of terrorism, as well as to the prevention and suppression of the proliferation of weapons of mass destruction. These conventions include, among others, the International Convention for the Suppression of the Financing of Terrorism and the Treaty on the Non-Proliferation of nuclear weapons.

DPMS are obliged to comply with the directives of the Competent Authorities of the State in relation to the agreements and conventions referred to above, including but not limited to Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions.

Because it is outside of the scope of these Guidelines to provide detailed guidance on this, reference is made to the guidance on TFS issued by the Executive Office for the Import and Export of Goods. Due to the significance, complexity and extent of the subject matter of international financial sanctions, it is deemed appropriate that this material be covered in depth in separate guidance materials.

70. ECONOMIC SANCTIONS

The United Nations Security Council (UNSC) holds the capacity to take action in seeking to maintain or restore international peace and security under the United Nations Charter, including by imposing sanctioning measures under Article 41, which encompasses a broad range of enforcement options that do not involve the use of armed forces. The UNSC has the authority to issue binding resolutions on United Nations (UN) member states.
The United Arab Emirates (UAE), as a member of the UN, is mandated to implement the United Nations Security Council Resolutions (UNSCRs), including those related to sanctions regimes. Consequently, through the Cabinet Resolution No. 74 of 2020, the UAE is implementing UNSCRs on the suppression and combating of terrorism, terrorist financing & countering the financing of proliferation of weapons of mass destruction, in particular, targeted financial sanctions (TFS) regimes as defined by the UN.
The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation of weapons of mass destruction (WMDs).

71. CONCLUSION

The Company and its employees fully comprehend the significance of the Sanction Screening Process and are committed to taking immediate action on Regulatory Notices, UAE-IEC lists, and Local Terrorist Lists. This proactive approach is essential to identify and address any potential threats related to money laundering and terrorism financing, ultimately safeguarding the integrity of the financial system.

In line with this commitment, the Company is dedicated to promptly reporting any suspicious activity or transactions to the relevant regulators and Executive Office. This applies to any suspicious incidents detected during the customer onboarding process, transaction processing, or periodic screening activities.

Furthermore, the Company will continuously enhance its Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) framework, particularly the sanctions screening program. This improvement will be carried out on a risk-based approach, taking into account emerging money laundering and terrorism financing threats as well as the evolving landscape of international sanctions regulations.

By adhering to these principles, the Company aims to strengthen its AML/CFT measures and contribute to the ongoing efforts in combatting financial crimes and ensuring regulatory compliance.

72. APPENDIX – 1: GLOSSARY

Glossary

AML	**Anti-Money Laundering**
AML/CFT/CPF	**AML/CFT/CPF Law: Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing, and Cabinet Resolution No. 134 of 2025 (its Executive Regulations).**
PF	**Proliferation Financing**
CFT	**Combating Financing of Terrorism**
CNMR	**Confirmed Name Match Report**
CDD	**Customer Due Diligence**
DPMS	**Dealers of Precious Metals and Stones**
EDD	**Enhanced Due Diligence**
KYC	**Know Your Customer**
CBUAE	**Central Bank of the United Arab Emirates**
FATF	**Financial Action Task Force**
UN	**United Nation**

EU	European Union
CO	Compliance Officer
EOCN	Executive Office for Control and Non-proliferation
NAS	Notification Alert System
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PNMR	Partial Name Match Report
SAR	Suspicious Activity Report
TFS	Targeted Financial Sanctions
MLRO	Money Laundering Reporting Officer
CID	Customer Identification Process
UIN	Unique Identification Number
UBO	Ultimate Beneficial Owner
FIU	Financial Intelligence Unit
STR	Suspicious Transaction Report
VASPs	Virtual Asset Service Providers
SDN	Specially Designated Nationals
NCCTs	Non-Cooperative Countries and Territories
TBML	Trade Based Money Laundering
WMD	Weapons of Mass Destruction