COMPLIANCE MANUAL & ANTI-MONEY LAUNDERING (AML) PROCEDURES

Version 1.0 / AUG 2023

Contents

**Nothing in this Compliance Manual is intended to limit or otherwise circumscribe additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback, whether direct or indirect, which may have been issued or may be published on occasion by any of the Supervisory Authorities in respect of the supervised institutions which fall under their respective jurisdictions, or in respect of any specific supervised institution.*

1. INTRODUCTION:

1.1 Purpose

- The DNFBP[1] Compliance Manual serves as a guide and reference for all employees of the AETERNO FZE (hereby referred to as the "Company" "AETERNO") on the expected standards and relevant DNFBP AML-CFT policies and procedures applicable to the company, members of its board of directors, management, employees, as well as its clients and vendors/suppliers.
- The Manual's purpose is to assist the company and its employees in gaining a clear understanding and the effective performance of their statutory obligations under the legal and regulatory framework in force in the United Arab Emirates.
- Throughout this Manual there are references to related AML-CFT policies, procedures and guidelines that provide further detail on the requirements and the evolving regulatory framework. Where possible, hyperlinks to these documents have been given for ease of reference.
- Following the DNFBP policies, procedures, and guidelines will help to advance and protect the long-term interest of both the company and its clients, as well as any entity with which it interacts (suppliers, commercial partners, etc.).
- The DNFBP service market is diverse, dynamic, and sizable in the UAE, and the AML-CFT rules andregulations that apply to them have been recently enhanced. This Manual and the AML-CFT policyand procedures referred to herein may be supplemented from time to time by the Supervisory Authority[2], Compliance Guidance Notes/Bulletins in line with improved regulatory guidelines would be circulated and employees should keep themselves updated.

Overview

AETERNO FZE is committed in compliance to, and strict practice of all regulatory requirements including those related to Anti Money Laundering by UAE and other competent world bodies. We comply with the regulations of world bodies which collectively set and enforce standards for Anti-Money Laundering and Counter-Terrorist financing policies and programs such as FATF, UN, The EU, The Organization of American States – The office of Foreign Assets Control (OFAC) and the Local Regulatory Authorities such as Central Bank of the UAE.

In UAE, the Central Bank of the UAE or more specifically the Anti-Money Laundering and Suspicious Cases Unit (AMLSCU) of the Central Bank is the regulatory body requiring the institution of AML rules. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing. The UAE has enacted two laws that serve as the foundation for the country's Anti Money Laundering (AML) and counterterrorist financing (CTF) efforts: Law No 4/2002, the Anti-Money Laundering law, and Law No. 1/2004, the counterterrorism law. Although the Anti-Money Laundering law criminalizes money laundering, it is administrative Regulation No. 24/2000 that provides guidelines for how financial institutions are to monitor for money laundering activity.

Violations

Failure to adhere to the policies and procedures contained in this Manual may result in disciplinary action taken by the firm, including the possibility of termination of employment. Violations of certain policies and procedures also may subject you to regulatory sanctions, criminal prosecution, and/or penalties imposed by regulators. Penalties may include monitory fines, temporary or permanent restrictions on your ability to engage in this business, sanctions, and imprisonment. The firm reserves the right to hold any employee personally liable for any loss or cost resulting from his/her failure to comply with the firm's policies and procedures and to report violations to the appropriate regulatory authorities as deemed required.

[1]The definition of a DNFBP as provided for in the relevant legislative and regulatory framework of the State are applicable to allsuch natural and legal persons in the following categories: Auditors and accountants | Lawyers, notaries and other legal professionals and practitioners | Company and trust service providers | Dealers in precious metals and stones | Real estate agents and brokers | Any other Designated Non-Financial Businesses and Professions not mentioned above.
[2] Federal and Local Authorities, entrusted by legislation to supervise Financial Institutions, DNFBP and Non-Profit Organizationsor the competent authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is notassigned by legislations.

1.2 Company Background

AETERNO FZE, referred to as “the company,” has a Gold and Precious Metal Refinery license from SAIF Zone (Sharjah Airport International Free Zone Authority – Sharjah, United Arab Emirates) issued in August 2023 under license no: 23916.

This manual is a compliance policy and framework designed specifically for the company’s activities and operations related to refining and export/import of precious metals and products.

1.3 Regulatory Background

- **Lead Regulators** – The company's primary regulator is SAIF Zone and MOE.

- **Supervisory Authority** – Have the responsibility of ensuring compliance to the Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML- CFT Decision") for Designated Non-Financial Businesses and Professions (DNFBPs).

- **Regulatory Framework and Guidelines**
  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. 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. Their implementation and enforcement arethe responsibility of the relevant regulatory and supervisory authorities in either the federal or local jurisdictions.

  Cabinet Decision No. (10) of 2019 concerning the implementation of Decree Law No. (20) of 2018On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML-CFT Decision") identifies Dealers in Precious Metals and Precious Stones as Designated Non-Financial Business and Professions (DNFBPs), when they engage in carrying out any single monetary transaction, or several transactions which appear to be interrelated, whose value is equal to or greater than AED 55,000, and subjects them to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates.

  The regulatory framework of the UAE is part of a larger international AML/CFT legislative and regulatory framework made up of a system of intergovernmental legislative bodies and international and regional regulatory organization i.e. i) The United Nations (UN), ii) The FinancialAction Task Force (FATF), iii) The Middle East and North Africa Financial Action Task Force (MENAFATF).

  In response to the regulatory expectations, DNFBPs, as mandated by the Supervisory Authority, are required to fulfil obligations which constitute the basis of an effective risk-based AML-CFT program. These obligations include:

  a) Identifying and assessing ML/FT (Money Laundering/ Financing of terrorism) risks
  b) Establishing, documenting, and updating policies and procedures to mitigate theidentified ML/FT risks
  c) Maintaining adequate risk-based customer due-diligence (CDD) and ongoing monitoring procedures
  d) Identifying and reporting suspicious transactions
  e) Putting in place an adequate governance framework for AML/CFT, including appointing an AML/CFT Compliance Officer, and ensuring adequate staff screening and training

f) Maintaining adequate records related to all of the above
g) Complying with the directives of the Competent Authorities and complying with recommendations.

Precious metals trading involves the trade, import, and export of non-manufactured items made from precious metals such as gold, silver, platinum, etc. A precious metals trader may be considered to be any natural or legal person (or legal arrangement), or their employee or representative, who engages, as a regular component of their business activities, in the trading of precious metals or scrap jewelry, whether in raw, cut, polished, or elaborated (mounted or fashioned) form. Trading in this context includes any of the following acts involving raw/rough or processed/finished precious metals:

- Import or export
- Purchase, sale, re-purchase, or re-sale (whether in primary, secondary, or scrap markets)
- Barter, exchange, or other form of transfer of ownership
- Loan or lease arrangements (e.g. sale-leaseback, consignment, or memorandum sales)
- Possession (whether permanent or temporary, for example, as part of a fiduciary, warehousing, collateral, or other safekeeping arrangement)

The above-referenced conditions are irrespective of whether the transaction is wholesale or retail; whether it is direct or indirect (such as through a broker or other intermediary); whether itis between natural or legal persons or legal arrangements; and whether the precious metals and jewellery are traded physically or virtually (for example, via certificates, on electronic exchanges, or via internet), irrespective of where or by whom the physical goods are warehoused,held in safekeeping, or delivered.

All Traders and Dealers of Precious Metals and Jewellery (PMS criteria's Appendix 7) which qualify as DNFBPs arerequired by the AML-CFT Law[3] and the AML-CFT Decision to fulfil certain obligations which constitute the basis of an effective risk-based AML/CFT program, in respect of covered transactions; the intent is to prevent the company and its activities from being exploited for the purposes of money laundering and/or the financing of terrorism.

[3]Under the AML-CFT Law and the AML-CFT Decision, companies and commercial entities are obliged to apply the required AML/CFT measures when they qualify as DNFBPs. This occurs whenever they carry out any single transaction, or series of transactions that appear to be related, whose monetary value equals or exceeds AED 55,000. This may include one or more transactions involving the same business relationship or customer, whether related to a single item or set of items; or it may also include one or more transactions which, in the judgment of the dealer, appear to be structured so as to avoid the established threshold.

2. GOVERNANCE, ROLES, AND RESPONSIBILITIES

2.1 Governance of these Procedures

The Compliance Manager and MLRO is responsible for establishing the procedures and ensuring that these are aligned with the regulatory requirements and guidelines issued by the Supervisory Authorities from time to time. The procedures must be reviewed at least once in two years (unless required otherwise) and any proposed changes must be submitted to Senior Management for approval.

The members of a DNFBP's senior management (together with the members of the board of directors, for those that have one) are ultimately responsible for the quality, strength, and effectiveness of the supervised institution's AML/CFT framework, as well as for the robustness of its compliance culture.

2.2 The Role of Compliance

2.2.1 Compliance Function

The role of the compliance function is as follows:

- Establish and maintain high compliance standards and a control framework
- Oversee the setting up of an effective compliance program and all the activities related to prevention of ML/TF
- Define internal policies, controls, and procedures to mitigate money laundering (ML), financing terrorism (FT), and other compliance-related risks in accordance with the nature and size of the business
- Identify, assess, monitor, and mitigate compliance and regulatory risk
- Provide proactive advice to management
- Provide training and instruction on standards and guidelines to all employees so they clearly understand the role they play in supporting compliance and flagging any risks (relevant to their level of involvement)
- Establish effective compliance monitoring arrangements
- Check the adequacy and effectiveness of implementation of these controls by line management
- Report any deficiencies to Senior Management and the concerned regulator as required
- Maintain relationship with the regulator(s)

2.2.2 Compliance Monitoring

Review of transactions that are carried out throughout the period of the business relationship, to ensurethat the transactions conducted are consistent with the information the DNFBP's have about their customer/client, their type of activity, as well as the risk they pose.

- **Transaction Monitoring** – undertaken on alerted unusual activities to identify potential cases of money laundering.
- **Name Screening** – screening of the potential client (at onboarding) against Country Watchlists, Sanctions lists, PEP database and Adverse Media data base in line with the Go AML/FIU requirements. The screening would be performed by Global Risk Profile.
- **Compliance Review** – Periodic risk-based reviews that are supported by tailored review scope.

These reviews address the adherence to the regulatory guidelines/procedures applicable for theDNFBP's and are also driven by the themes identified at business, trends/risks derived from the business dashboards/risk metrics.

2.2.3 Responsibilities of a Compliance Officer

Appoint a compliance officer independent of the business. The compliance officer shall have the appropriate competencies and experience and under his or her own responsibility, shall perform the following tasks:

- Detect transactions relating to any crime
- Scrutinize and study records, receive data concerning Suspicious Transactions, and take decisionsto either notify the Financial Intelligence Unit (FIU) or maintain the transaction with the reasonsfor maintaining while maintaining complete confidentiality
- Review the company procedures relating to combating crime and illegal activities and their consistency with the Decretal-Law 2018 No. (20) and the present Decision 2019 No (10); assess the extent to which the institution is committed to the application of these rules and procedures, propose what is needed to update and develop these rules and procedures
- Prepare and submit semi-annual reports on the above points to senior management and send a copy of that report to the relevant Supervisory Authority enclosed with senior management remarks and decisions
- Prepare, train, and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Activities
- Provide Supervisory Authority and FIU with all relevant data, and allow their authorized employees to view the necessary records and documents that will allow them to perform their duties
- All regulatory breaches are to be reported by Compliance to the supervisory authorities (regulators)in accordance with the applicable requirements

2.3 Division of Responsibilities and The Three Lines of Defense

For adequately covering the AML-CFT risk management, the 'Three Lines of Defense Model' is recognized as the most effective to protect the organization from ML/FT vulnerabilities.

2.3.1 The First Line of Defense – Business

All staff members are responsible for managing Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) risks within the scope of their direct organizational responsibility and must ensure compliance with the requirement of these procedures. The Business forms the first line of defense and includes the front office/sales/service teams responsible for Client Onboarding / Know your Customer(KYC) / Client Due Diligence (CDD) / Off boarding.

2.3.2 The Second Line of Defense – Compliance

The second line of defense should be independent from the Business (i.e. origination, trading, and sales functions) to ensure that the necessary balance and perspective is brought in; it holds the authority to challenge the First Line activities in the event of the First Line deviates from their roles and responsibilities as the First Line of Defense for AETERNO FZE. The Second Line is responsible for AML-CFT compliance and monitoring, setting up policies, providing advice and reporting suspicious transactions. Liaison with the Regulator, Sanctions advisory, Investigations, and Suspicious Activity

Report are also within their purview.

Appointment of an AML/CFT compliance officer with the appropriate competencies and experience to perform the statutory duties and responsibilities associated with the role is required.

2.3.3 The Third Line of Defense – Audit

Audit as the Third Line of Defense has no management responsibilities for any of the activities it examines, it is therefore able to provide independent assurance on the effectiveness of the First Line and the Second Line. Audit has unrestricted access to all records, information, personnel, and physical properties that are relevant. Audit reports to the Board provide visibility on the effectiveness of the existing controls.

An independent audit function to test the effectiveness and adequacy of the internal polices, controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organizations is required. The independent audit function should be appropriately staffed and organized and should have the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the ML/FT risks to which the supervised institutions are exposed, and with the nature and size of their businesses. Adequate measures to obtain the necessary capabilities from qualified external sources should be taken as required.

Periodic inspection and testing of all aspects of the company's AML/CFT compliance program, including ML/FT risk assessment and mitigation measures, and customer due diligence policies, procedures, and controls, must be incorporated into the regular audit plans.

2.4 Responsibilities of Senior Management/Board

The quality, strength, and effectiveness of the institution's AML/CFT framework, as well as the robustness of its compliance culture is one of the key responsibilities to be demonstrated by Senior Management and the Board of Directors (should it exist) of the company. They are therefore accountable as follows:

- Responsible for implementing systems and controls and demonstrating governance through appointment of an independent audit function, qualified compliance officer, in addition to putting in place governance and controls in line with the size and complexity of the business
- Approving the policy, procedures, and controls best suited for the company, covering but not limited to, AML/CFT, staff screening and recruitment, data protection, and record retention
- Oversight of key elements of the AML/CFT compliance program covering but not limited to:

  onboarding, retaining high-risk customers, customers from countries deemed as having an 'Elevated Risk', review of the compliance officer's reports (Quarterly or at a minimum semi-annually)
- Ensuring AML-CFT directives of the competent authorities (local / international as communicated through the supervisory authorities) are adequately followed and applied

Senior management are also expected to ensure a clear and effective separation of AML/CFT responsibilities from those related to the day-to-day management of the businesses, including but not limited to sales and customer business relationship management functions.

If due to the small size of the organization, that should not be possible, or there exists some form of conflict, additional measures to enhance assessment of the application of the AML/CFT guidelines and procedures need to be emphasized through independent audit controls (function).

2.5 Small and Mid-Size Business Governance Challenges and Risk Mitigation

Given the size of the firm and where a single person operation exists, whereby an individual undertakes multiple roles and responsibilities in the course of day-to-day business activities, and it is not possible to maintain a clear separation of duties or functions. This does not exempt the company from fulfilling its obligations under the AML-CFT Law and AML-CFT decisions, as applicable.

- If adequate separation of responsibilities is not possible due to the small size of the firm necessary steps have been taken to ensure that AML/CFT policies and procedures (particularly those pertaining to Customer Due Diligence, the identification of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and International Sanctions) have been clearly formulated, documented; these are adhered to during the establishment and ongoing monitoring of business relationships and the carrying out of transactions.
- The rationale for any policy and/or procedural exceptions being made with any additional ML/FT risk-mitigation measures implemented are properly recorded and retained in accordance with the statutory record-keeping requirements.
- As the firm is unable to ensure independence, clear and effective separation of AML/CFT responsibilities from those related to the day-to-day management of the businesses, additional measures to enhance the application of the independent audit controls must be emphasized by way of some of the below measures:
    - Incorporating the audit of policies, procedures and records related to exceptions made by the company, as part of their audit plans and/or their service-level agreements with their external providers of independent audit services
    - Biannual Independent audits

3 Record Retention

It is essential that adequate, orderly, and up to date records are maintained, which must include, but are not necessarily limited to:

- Customer Due Diligence Information
- Transactions effected for/by the client
- Transactions executed or processed by the organization
- Company information specifically for administrators and liquidators involved in the dissolution of a company
- Record retention process at vendors in the event that CDD services are outsourced
- Ongoing monitoring of clients' business transactions undertaken
- Suspicious Transactions Reports (STRs)
- Compliance, Audit reports, and Board decisions/resolutions

Obligations and timeframe for the retention and availability of records is at least five (5) years from:

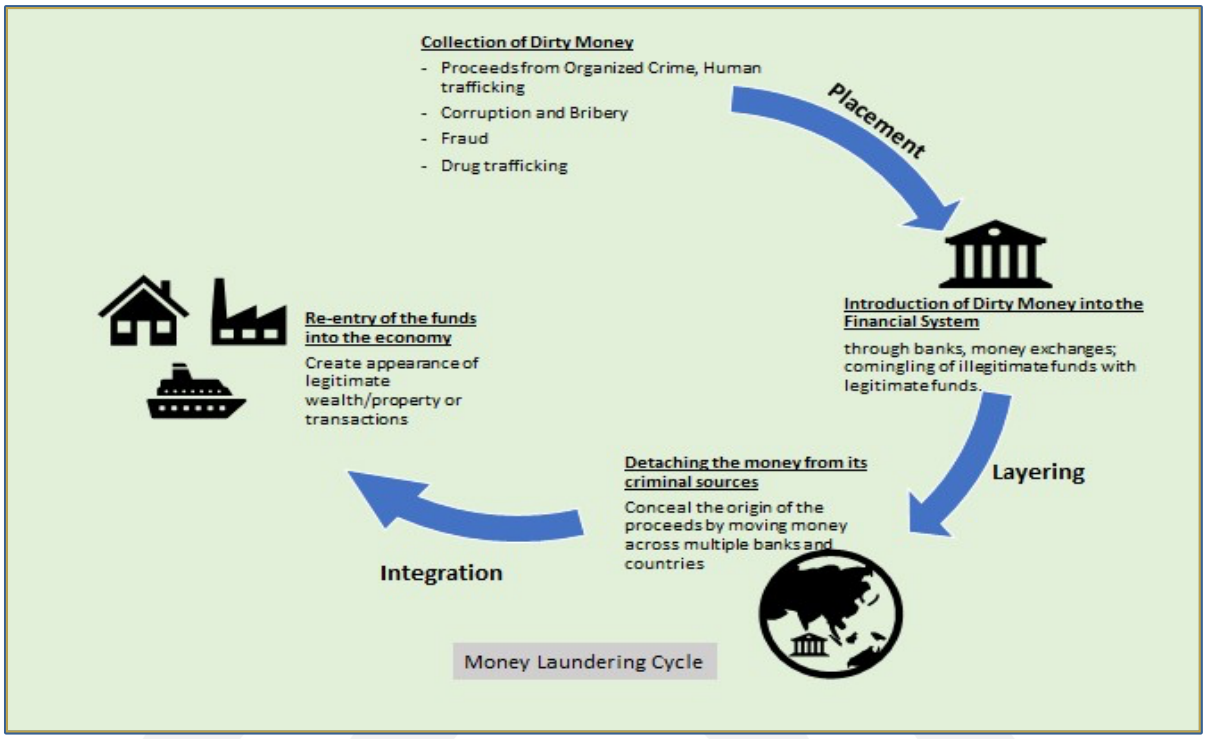
- Completion of the transaction or the termination of the business relationship or the closing of a customer's account with the company
- Completion of an inspection of the records by the Supervisory Authorities or the issue date of afinal judgment.
- Liquidation, dissolution, or any other form of termination of a legal person or arrangement

4 Money Laundering & Financial Crime Prevention

- As a designated non-financial business and profession, AETERNO FZE is committed to the cause of denying criminals and terrorists access to the financial system and its tools and is determined to comply with the applicable AML-CTF laws and regulations issued by the supervisory authorities.
- It is imperative that staff who perform KYC (Know your Customer), exercise vigilance and assist the company in preventing its involvement in any transaction that presents money laundering and terrorist financing risks; also review if the clients are from a jurisdiction/country which is associated with higher level of corruption and the risks associated. Financial Crime Risk if not effectively mitigated, poses significant legal, reputational, and regulatory risks to AETERNO FZE.

4.1 Money Laundering Cycle

All staff are required to appreciate and recognize the typical stages involved in money laundering such that they remain watchful of any ill intent that may fall within their line of sight. The procedures carry a detailed explanation of these stages.



4.2 Know Your Customer (KYC) and Client Due Diligence (CDD)

- KYC and CDD are critical elements of the company's framework for managing financial crime risks. By understanding its clients and reviewing the necessary documentation, the company can determine and mitigate the level of financial crime risk that they may pose.
- In line with the AML-CFT guidance for DNFBP's, AETERNO FZE has adopted a robust risk-based approach in differentiating/categorizing clients presenting different levels and types of risks. Risk mitigation and control, including and not limited to the need or frequency of periodic review of customers, are determined in accordance with the risk profile that the customer presents.
- Staff must familiarize themselves with the procedures on CDD.

4.3 Sanctions

Staff are to ensure that the company does not deal or transact with individuals, countries/jurisdictions, and entities/organizations that are sanctioned, and must comply with the directive of the supervisory authority on the same and in line with the sanctions list.

- Familiarize themselves with the Sanctions.

- Ensure clients' backgrounds are checked against the sanction list before completing a transaction with a client.

The sanctions list should be referred to at https://www.uaeiec.gov.ae/en-us/united-nations-security-council-sanctions. Updates from the Supervisory Authorities on the sanctions list should be tracked by the DNFBP by reaching them through the following email: sanctions@uaeiec.gov.ae

4.4 Suspicious Activity

- Defined as transactions or funds of which the staff has 'reasonable grounds' to suspect as constituting either proceeds of crime or being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organization or being intended to be used in an activity related to such crimes.
- Staff must take adequate care to ensure that the client/counterparty should not be tipped off on the suspicion and the same should be recorded, escalated, and reported to the compliance officer/manager.
- Compliance officer is obligated to report to the Financial Intelligence Unit (FIU) suspicious transactions (STRs) and any additional information required in relation to them, and to maintain up-to-date indicators that can be used to identify the suspicion of a crime involving ML/FT.

5 Statutory Prohibitions

All staff are expected to act with vigilance to guard against the following activities prohibited under law:

- Conducting any financial or commercial transactions, or keeping any accounts or customer under an anonymous or fictitious name or by pseudonym or number
- Establishing a relationship or executing any transaction in the event they are unable to completeadequate Customer Due Diligence
- Dealing with Shell Banks in any form
- Not reporting suspicious activities under any pretext
- Issuing bearer shares and warrants

6 Employee Training

All staff have the individual responsibility to undertake requisite training and obtain appropriate knowledge relevant to their job role to ensure that they have the necessary skills and know-how to undertake their roles effectively. While training is applicable for all staff members, there are certain job categories which are considered to be at the forefront of implementing and executing the AML-CFT procedures, and hence would need greater levels of engagement and training by the Compliance officer.

For the staff training the following need to be kept in mind:

- Result of the National Risk Assessment to appreciate top risk
- Understanding of AML-CTF risk based on the nature and the size of the industry the firm is in
- Ability to Identify and assess AML-CTF risks(periodic assessment of staff competencies)
- Take adequate steps to mitigate the risks identified(appreciation of the core risks)
- Escalation and reporting protocols
- New Joiners training should be completed on their joining before they are allowed on the job Senior

Management is responsible for:

- Ensuring that appropriate training and annual refresher is taken by all staff

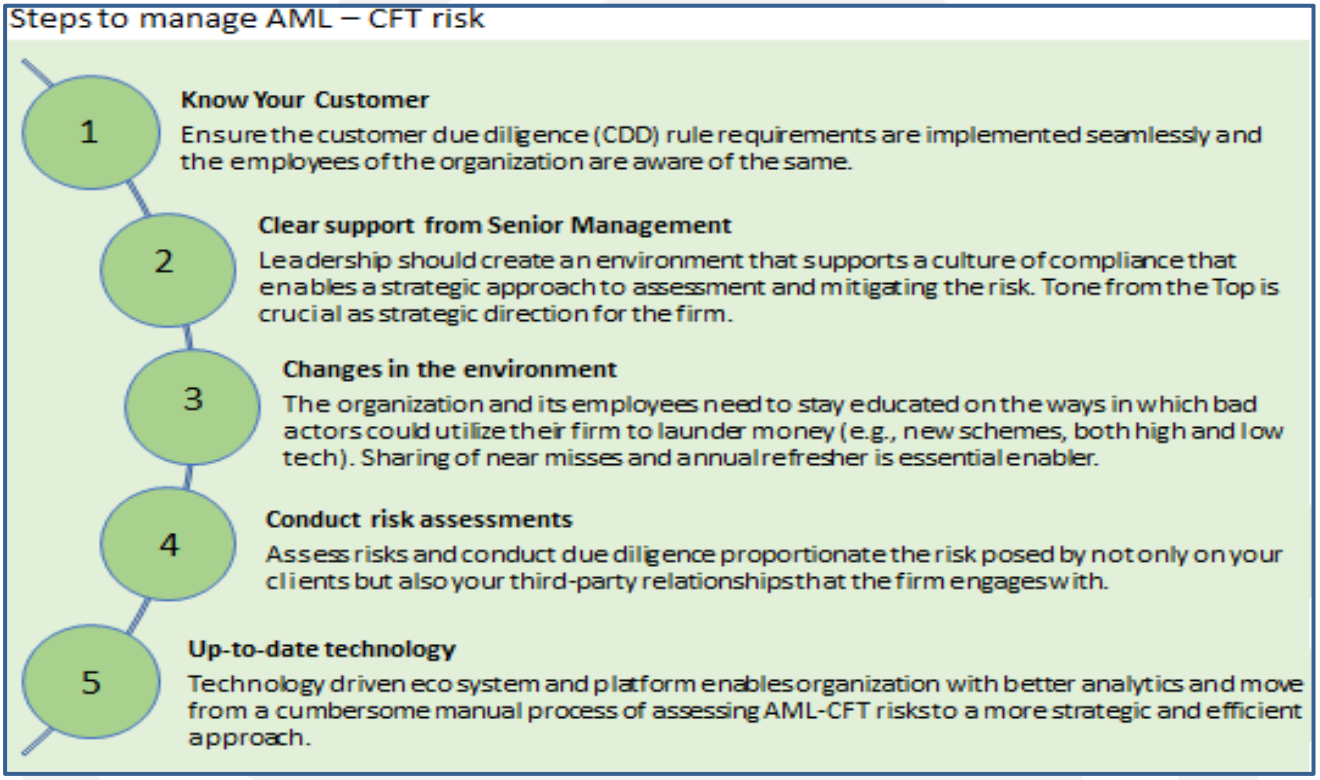
- Review with the compliance officer the adequacy of the training
- Ensure that training records are maintained to evidence trainings performed

7 Wrap-up

While attempt need to be made to obviate money laundering and terrorist financing risk, a risk-based approach (RBA) has been recommended for the Identification, Assessment, Understanding, and Mitigation of the risks posed.

7.1 Steps to Manage AML – CTF Risk

The critical steps in the management of the AML – CTF compliance have been threaded below as a summary.



ANTI-MONEY LAUNDERING PROCEDURES

CHAPTER 1 : INTRODUCTION TO MONEY LAUNDERING AND TERRORIST FINANCING

1.1. What is money laundering?

Money laundering is generally defined as the process used to 'disguise' the illegal source money willfully, knowing fully well that the "funds" are the proceeds of criminal activities (such as fraud, activities of organized crime such as illegal arms sale, drug trafficking and tax evasion). Transferring or moving these proceeds or conducting any transaction with the aim of concealing or disguising their illegal source is called 'Money laundering'.

This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. By making the money look like it comes from a legitimate source, they can cover their tracks and avoid detection. Money laundering makes it harder for authorities to detect 'dirty' money, stop crime, prosecute criminals, and seize illegally earned money and assets.

The AML-CFT Law define "funds" as "assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets." Therefore, for an act of money laundering to be considered as such, it is not necessary for cash to be involved.

1.2. Process of money Laundering:

The process often involves a complex series of transactions that are difficult to separate. Typically, money laundering has been described as a process which takes place in three distinct stages: placement, layering, and integration.

1.2.1. Stage I - Placement

Placement is the stage at which criminally derived funds are introduced into the financial system. The funds will then be placed into circulation through financial institutions, casinos, currency exchanges, and other businesses both locally and abroad. The process of placement can be carried out through many methods including:

- Currency smuggling – this is the physical movement of currency and monetary instruments out of a country
- Currency exchanges – purchasing of foreign exchange with illegal funds
- Securities brokers – can facilitate the process of money laundering through structuring large deposits of cash in a way that disguises the original source of the funds
- Blending of funds – Co-mingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurant
- Asset purchase – the purchase of assets (including precious metal & stones) with cash is a classic money laundering method. The major purpose is to change the form of the proceeds from conspicuous bulk cash to some equally valuable but less conspicuous form

1.2.2. Stage II – Layering

This involves the separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds. The purpose of this stage is to make it more difficult for law enforcement agencies to detect and uncover a laundering activity. Known methods include:

- Converting cash into monetary instruments – once the placement into the financial system has beensuccessful, the proceeds can then be converted into monetary instruments. This involves the use of bankers' drafts and money orders
- Moving funds from one financial institution to another or within accounts at the same institution
- Placing money in stocks, bonds, or life insurance products
- Selling material assets bought with cash – assets that are bought with illicit funds can be resold locallyor abroad whereby the assets become more difficult to trace and thus seize

1.2.3. Stage III - Integration

Integration is the final stage at which the 'laundered' property is re-introduced into the legitimate economy, whereupon such monies now appear to be normal business or personal transactions. Exampleof known methods used include the following:

- Property dealing – the sale or transfer of property to reintegrate laundered money into the economyis a common practice amongst criminals. Many criminal groups will use shell companies to purchase property and thus the proceeds of sale would appear to be legitimate
- Front companies and false loans – front companies are incorporated in countries with corporate secrecy laws and criminals lend themselves their own laundered proceeds in an apparently legitimatetransaction
- False import/export invoices – the use of false invoices by import/export companies has proven to be a very effective way of reintegrating illicit proceeds into the economy. This involves the overvaluation of entry documents to justify the funds which are later deposited in domestic banks and/or the value of funds received from exports

1.3 What is Terrorist Financing

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.

Terrorist financing may occur through methods that are similar to money laundering; however, unlike money laundering where the source of funds is always unlawful, in terrorist financing the source may belegitimate but the funds themselves are intended to be used for unlawful purposes.

The law designates financing of terrorism as a criminal offence. Being aware and participating or facilitating such financing is a crime and is against firm's policy, some characteristics of terrorist financing that can make it difficult to detect include the following:

- Terrorists may finance attacks through simple transactions which involve relatively small amounts ofmoney and may be indistinguishable from normal activity
- Terrorists may finance attacks using both unlawful and lawful sources of funds including charitable donations

Terrorist financing can be difficult to identify, it is therefore critical that all employees escalate any suspicions of potential terrorist financing to the Compliance Officer at the first opportunity.

Like the financing of terrorism, the AML-CFT Law designates the financing of 'Illegal Organizations' as a criminal offence.

1.4 Applicable AML Laws & Rules

The UAE is deeply committed to combating money laundering and the financing of terrorism and illegal organizations. Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection, and deterrence of financial crimes by implementing the internationally accepted AML/CFT standards recommended and promoted by FATF, MENAFATF and the other FSRBs (FATF-Style Regional Bodies), as well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

National Risk Assessment (NRA) to identify and assess the ML/FT threats and inherent vulnerabilities to which the country is exposed have been performed and the federal legislative and regulatory framework have been enhanced by the introduction of the new AML/CFT Law, Cabinet Decision and Guidelines which have been considered for the purpose of these procedures.

The NAMLCFTC is responsible for overseeing the national risk assessment process (NRA) https://www.namlcftc.gov.ae/en/national-risk-assessment.php

1. Decree Federal law No. (20) of 2018 on Anti-Money Laundering and combating the financing of terrorism and illegal organizations.

2. Cabinet Decision No. (10) Of 2019 concerning the implementing regulation of Decree Federal law No. (20) of 2018 on Anti-Money Laundering and combating the financing of terrorism and illegal organizations.

6. Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations - Guidelines for Designated Non-Financial Businesses and Professions.

7. Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations - Guidelines for Designated Non-Financial Businesses and Professions - Supplemental Guidance for Dealers in Precious Metals and Stones.

All Federal laws issued by the UAE are available on the Ministry of Justice's Legislation Portal.

The above list may not be all encompassing and may also be subject to change by relevant Federal authorities.

Other Relevant Laws: International Tax Issues and compliance

In the process of carrying out a customer risk assessment, consider and assess the tax crime risk associated with the customer and factor such risks into the overall risk assigned to that customer. Many of the factorsdescribed for higher risk customers could also be an indicator of potential tax crimes, for example, the use of complex or unusual corporate structures, the customer's business not being located where the customer lives (without adequate explanation), unusual customer interface or reluctance by the customer to communicate directly with the relevant person or the customer being unable or unwilling to disclose the source of funds and wealth.

Under the Federal AML legislation, company and individual employees may be criminally liable for the offenceof money laundering if it/they intentionally commits specified acts in relation to funds which it/they knew are the proceeds of crime.

CHAPTER 2. Client Risk Assessment

A Risk-Based Approach to CDD

2.1 Introduction

The company applies a risk-based approach for the assessment of any business relationship or transaction regarding the specific money laundering risks which it may present.

The Risk-Based Approach (RBA) requires a risk assessment of the customers/transaction to determine the risk profile and the corresponding due diligence needs. The risk-based assessment process is dynamic and the information obtained from the client across the risk factors will be the principal drivers of the same.

2.2 Key Tennent's of Risk Based Approach

Essentially, the risk-based approach requires an assessment by considering the following risk factors:

RISK FACTORS

<table>
<tr>
<td>

CUSTOMER RISK

- **Enterprise/Business Level Risk:**
  - Target Market
  - Size & Variety of Customer Base
  - Business Model
  - IT System Capabilities
- **Client/Relationship Level Risk:**
  - Overall Background and reputation(PEP)
  - Beneficial Ownership(BO)
  - Ultimate Beneficial Ownership(UBO)
  - Source of Funds

</td>
<td>

Country/Geographic Risk:

- Regulatory/Supervisory Framework
- Reputation/Corruption(PEP) and Transparency risks
- International sanctions
- Customer Profile mismatch

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

Product, Service & Transaction Type Risk:

- Complexity of products, services & transactions
- Transaction mode – Cash/CreditCard/Cheque
- Existing Typology risk
- Transparency and transferability
- Size/Value and adequacy of controls

</td>
<td>

Channel Risk:

- Non face to face (internet/phone) risk
- Intermediaries, third party introducers
- Money value transfer, transaction intermediaries

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

2.3 Risk Assessment

2.3.1 Relationship Level

The company undertakes a risk assessment based on the client/relationship level risk at the core while keeping the other tenets in mind and assigns the client a risk rating which would be proportionate to the client's money laundering risks. The client risk assessment must be completed on the client onboarding form prior to undertaking CDD for new clients in order that the correct risk rating is ascertained. This then governs the extent of CDD required, and whenever it is otherwise appropriate for existing clients. When undertaking a client/customer risk assessment, the firm must:

- Obtain all the basic information on the purpose and intended nature of the business relationship
- Identify the Ultimate Beneficial Owners, Beneficial Owners, Directors, and the Authorized Signatories

- Take into consideration the nature of the client, its ownership and control structure, and its Ultimate Beneficial Ownership, and Beneficial Ownership. When assessing the nature of the client, the company should consider factors such as the legal structure of the client, the client's business or occupation, the location of the client's business, as well as the commercial rationale for the client's business model
- Take into consideration the client's country of origin, residence, nationality, and place of incorporation or
  place of business. Sanctions and PEP risk also need to be assessed and factored in
- How the client was introduced to firm (i.e. is the client an existing customer of the company, or a new customer?);

The company acknowledges that a risk-based approach does not release it from its overall obligation to comply with anti-money laundering legislation.

2.3.2 Business risk assessment

The company is required to identify and assess money laundering risks to which its business is exposed, taking into consideration the nature, size, and complexity of its business at its core keeping the other risk factor tenets in mind. The company need to identify and assess the money laundering risks, to the extent relevant, and any vulnerabilities relating to:

- Types of client and their activities
- Countries or geographical areas in which it does business
- Political exposure and corruption
- Distribution channels and business partners
- Complexity, volume, and mode of transactions (Cash vs Non-Cash)
- Development of new products and new business practices, including new delivery mechanisms, channels, and partners
- Use of new or developing technologies for both new and pre-existing products
- Types of products, services, and activity profiles

Note: Cash Transaction

AETERNO FZE, as a matter of practice, will continue to diminish the instance under which we accept receipt of cash for purchases made at their counter. While customers are encouraged to pay through non-cash means, it is acknowledged that the organization - as part of the trade practice - needs to cater to clients making purchases on cash. To actively manage the risk associated with the same, the below thresholds and steps are to be strictly followed:

- Cash Transactions greater than or equal to AED 55,000/- with adequate justification must first be approved by the Manager & CO of the firm (Appendix 8).
- The company, while performing CDD, will conduct appropriate due diligence to establish and corroborate the possible source of funds (e.g. evidence of withdrawal from customer's own account, for cash intensive businesses bank statement reflecting sizable deposits as part of BAU (business as usual), exchange house receipts, tourists on travel visa) for all cash transactions. The justification and approval need to be articulated at the time of executing the transaction.

Reporting requirements (mandatory) for cash transactions equal to and greater than AED 55,000:

- Transactions with resident individuals: The CO will register the transaction information along withidentification documents i.e. Emirates ID or Passport in the Financial Intelligence Unit's ("FIU") GoAML platform using the 'Dealers in Precious Metals and Stones Report'.
- Transactions with non-resident individuals: The CO will register the transaction information alongwith identification documents i.e. ID or Passport in the Financial Intelligence Unit's ("FIU") GoAML platform using the 'Dealers in Precious Metals and Stones Report'.
- Transactions with entities / companies: The CO will register the transaction information along with the trade license and identification documents (Emirates ID or Passport) of the person representing the company in the Financial Intelligence Unit's ("FIU") GoAML platform using the 'Dealers in Precious Metals and Stones Report'.

**Records of the above transactions reported have been specifically mandated for a period of 5years.*

While the responsibility of uploading the document is with the Compliance Officer, all frontline staff are responsible for compliance of the requirements as a process.

Find hereunder link of video detailing the process for uploading these transactions:
https://www.youtube.com/watch?v=pcJvG63wF4g&list=PL7ZJRXOjiDmXSkeyW0Re6kWuWtrnjAYWw

2.3.3 PEP and Sanctions Risk:

2.3.3.1 Politically Exposed Persons ('PEPs')

Individuals who have (or have had) a high political profile or hold (or have held) public office may pose a higher AML risk. There is a possibility that individuals holding such positions may misuse their power andinfluence for personal gain or advantage, or for the gain or advantage of their immediate family or close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the client/customer into a higher risk category.

Examples of such activity may include bribery and corruption, embezzlement, fraud, money laundering, racketeering and misappropriation of state funds and assets. Consequently, relationships involving PEPs present increased legal, regulatory, financial, and reputational risks to the company.

PEPs are defined as follows:

A natural person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, whether in the state or elsewhere, including but not limitedto:

- Direct family member of PEP (spouses, children, spouses of children, parents)

- Associates known to be close to the PEP (Individuals having joint ownership/individual rights in a legal person or arrangement or any other close Business Relationship with the PEP)

Some examples of PEP's are:

- a head of state or of government
- senior politician
- senior government
- judicial or military official
- ambassador
- senior person in an International Organization
- senior executive of a state-owned corporation
- an important political party official
- a member of senior management
- an individual who has been entrusted with similar functions such as a director or a deputy

director These definitions do not include middle ranking or more junior individuals in the above categories.

Where a Client relationship is maintained with a PEP, detailed monitoring and due diligence procedures should include:

- Analysis of any complex structures, for example involving trusts or multiple jurisdictions
- Appropriate measures to establish the source of wealth (making reasonable investigations into the individual's professional and financial background prior to becoming a PEP) and source of funds (to establish legitimacy)
- Development of a profile of expected activity for the business relationship in order to provide a basis for transaction and account monitoring
- Senior management approval for the account opening
- Regular oversight of the relationship with a PEP by senior management

It is considered that after leaving office a PEP may remain a higher risk for money laundering if such a person continues to exert political influence or otherwise pose a risk of corruption. Therefore, a person flagged as a PEP shall continue to be classified as such for a minimum of 3 (three) years after they leave the PEP classified position. The removal of a person from the PEP list will require firm senior management approval.

2.3.3.2 Sanctions (Targeted Financial Sanctions)

The company must establish and maintain effective systems and controls to ensure that, on an ongoing basis. it is properly informed as to take reasonable measures to comply with the relevant resolutions or sanctions issued by the United Nations Security Council ('UNSC').

- Carrying on or about to carry on an activity
- Holding or about to hold money or other assets
- Undertaking or about to undertake any other business whether or not arising from or in connection with the above, for or on behalf of a Person, where such carrying on, holding or undertaking constitutes or may constitute a contravention of a relevant sanction or resolution issued by the UNSC

Any such notification must include a description of the relevant activity (as described above) and the action proposed to be taken or that has been taken by the company with regard to the matters specified in the notification. To assist in reducing the risk of a breach of this requirement, the company will utilize the Global Risk Profile, potentially also using other companies such as World Check. Global Risk Profile monitors various sanction, watch, and regulatory law and enforcement list, including OFAC, EU, UNSC and UK HMT; https://www.uaeiec.gov.ae/en-us/united-nations-security- council-sanctions (updates from the Supervisory Authorities on the sanctions list should be tracked by the DNFBP to reach them through id "sanctions@uaeiec.gov.ae"). The names of the client, its directors, and shareholders will be input into the Global Risk Profile database by the compliance officer to determine whether they match the names appearing on a sanction list; true match confirmed by the CO/MLRO results in that party being declined for business and ANY transaction; all such cases will be maintained as part of the business denied register/tracker. The search also determines whether the directors or shareholders have been classified as PEPs.

The principal obligations of the organization as a DNFBPs under Cabinet Decision No 74 of 2020 concerning the UAE List of Terrorists and the Implementation of UN Sanctions Council Decisions relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of MassDestruction, and the Relevant Regulations, necessitate the following categories of actions:

- Maintaining a continuously up-to-date awareness of the persons and organizations listed in the relevant Sanctions Committees lists and comparing these on an ongoing basis with their customer databases
    - **Registering** at the Executive Office website to receive automated email notifications: https://www.uaeiec.gov.ae This registration is aimed to help DNFBPs to receive updated andtimely information about the listing and de-listing of individuals or entities in the Local Terrorist List and in the UN List

- Ensuring, prior to entering into business relationships or conducting any transactions with natural orlegal persons or legal arrangements, that such persons or organizations are not included in the relevant Sanctions List
    - **Screening:** Regularly screen their databases and transactions against names on lists issued by the UN Security Council, the Sanctions Committee or the Local Lists, and also immediately when notified of any changes to any of such lists, provided that such screening includes the following listed:
        - Existing customer databases
        - Names of parties to any transactions
        - Potential customers
        - Beneficial owners
        - Names of individuals or entities or indirect relationships with them
        - Customers before conducting any transactions or entering a business relationship withany person
        - Directors and/or agents acting on behalf of the client/customer (including individuals with powerof attorney).

- **Freezing** (or unfreezing when so instructed by the Competent Authorities) the Funds of listed personsor organizations, which the supervised institutions hold, have access to, or otherwise control
    - Implement freezing measures, without delay (immediately or ideally within 24hrs), and without prior notice to the Listed Person immediately when a match is found through the screening process

- **Immediately reporting** to the Supervisory Authorities as per requirements of the relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Lists on :
    - Identification of funds and actions that have been taken, including attempted transactions
    - Detection of any match with listed persons or entities including current, previous customers or any occasional customer it dealt with, details of the match data and actions
    - If no action has been taken due to a false positive, and the inability to dismiss such false positive through available or accessible information
    - Information relating to funds that have been unfrozen, including their status, nature, value, and measures that were taken in respect thereof, and any other information relevant to suchdecisions

CHAPTER 3. KNOW YOUR CLIENT/CUSTOMER ('KYC') AND CLIENT DUE DILIGENCE ('CDD')

3.1 Introduction:

KYC (Know Your Customer) checks are the initial background checks that should be carried out as part of the firms risk-based approach. The KYC process involves the verification of the customer's identity, using documents like photographic ID, proof of date of birth, and proof of address. Through the KYC process the company identifies its clients/customer and ascertains relevant information before agreeing to rendering services to them.

CDD (or Customer due diligence), is a longer process which begins once primary information on the client is collected on the customer before onboarding and continues even after the customer has been onboarded. CDD is the process of a business verifying the identity of its clients and assessing the potential risks to the business relationship and includes checks like sanctions and PEP screenings.

Both KYC and CDD are crucial aspects of AML compliance and are the critical first step to initiate a relationship with a client/customer. Regulated firms must identify and verify anyone they work with, to ensure they don't unknowingly become involved with a business or individual with a history of financial crime. Any inadequacy of KYC and CDD standards can expose the company to serious business operational risks, as well as control risks.

3.2 Know Your Customer:

It is the company's policy not to open or to maintain anonymous client relation, or accounts, in fictitious names. If the company is unable to verify the identity of the customer or Ultimate Beneficial Owner & Beneficial Owner, it will not open client account, establish a business relationship, or carry on processing / undertaking the assignment or transaction. Knowing the persons with or for whom the client acts or proposes to act consists of several elements:

- Personal details: The company should obtain and verify details of the Client which include their true full name or names used and their current permanent address through passports, government identification cards, etc.
- Proof of address: The company should obtain and verify details of the Client's address through utility bill, voter's registration card, trade license, on-site Personal visit, etc.
- The nature and level of business to be conducted: The company must ensure that sufficient information is obtained regarding the nature of the business that the Client expects to undertake along with any expected or predictable pattern of transactions. This information should include:
    - The purpose and reason for opening or establishing the business relationship.
    - The anticipated level and nature of the activity that is to be undertaken in the proposed firm(not only in terms of fees); and
    - The various relationships of signatories to the account and the underlying Ultimate BeneficialOwners & Beneficial Owners.

- The origin of funds (SOF-Source of Funds): [Please refer to "Note: Cash Transaction" above] The company needs to identify how all payments are to be made, from where, and by whom. This process involves understanding where the funds for a specific service or transaction

will come from (e.g. aspecific bank account held with a specific financial institution) and whether that funding is consistent with the customer's source of wealth. The best way of understanding the source of funds is by obtaining information directly from the source (example: bank statement). The company should keep appropriate evidence of how they were able to understand the source of funds. Examples of this include a copy of the customer account opening form, customer questionnaire, or a memo of a call with the relationship manager at a financial institution, etc. All payments should be recorded to provide an audit trail.

- The Source of Wealth (SOW): [Refer to the "Note: Cash Transaction" above]
  The company should establish the Source of Wealth or income, including how the wealth was acquired, to assess whether the wealth is consistent with what would be expected from the individuals source of income and whether this constitutes any grounds for suspicion in the event the SOW can't be corroborated. At times the information on the client's SOW is publicly available (i.e. published accounts or balance sheet of company or in a reputable news source). A dollar-for-dollar account of the customer's wealth is not required if build-up can be adequately substantiated. The customer's SOW should be clearly articulated.

  Understanding a customer's SOF and SOW are important for the purposes of undertaking ongoing due diligence as required depending on whether it is an individual making a onetime or regular purchases or a legal entity (company).

CHAPTER 4: CUSTOMER DUE DILIGENCE (CDD)

4.1 CDD:

In line with the AML-CFT law the company recognizes the need for the risk-based approach (RBA) to CDD while taking into consideration the various risk factors and the results of the national risk assessment.

The extent of due diligence undertaken on the customer by the company will be proportionate to the risk posed by the customer. However, each client will have to undergo CDD. Identified low risk leads to Simplified Due Diligence (SDD) for the client, while an Enhanced Due Diligence (EDD) is for high risks identified customer as a part of the risk assessment.

Each customer's ML/FT risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behavior. The appropriate level of due diligence will then be applied in keeping with the specific situation and risk indicators identified.

I. High Risk Clients

Higher-risk clients may include:

- Non-face-to-face business relationships or transactions
- Businesses that are cash-intensive
- Clients from Countries with Elevated Risk
- Politically Exposed Persons ('PEPs')
- Client on whom a SAR has been reported

- Situations where a person is able to hide behind corporate structures such as limited companies,trusts, special purpose vehicles and nominee arrangements
- Discretionary trusts and Charitable trusts
- Where unlimited third-party funds can be received without evidence of the identity of the thirdparty.

Where the company confirms that a client is considered higher-risk, consideration is given to the additional KYC and monitoring requirements that might be necessary to compensate for the enhanced risk such as:

- Requiring additional KYC due diligence documentary evidence
- Taking supplementary measures to verify or certify the documents supplied
- Performing direct mailing of account opening documentation to a client at an independently verified address or
- Establishing telephone contact with a client prior to opening the account

II. Countries with Elevated Risk

The geographical location of a client may affect the risk assessment countries with elevated risk may include:

- Those without adequate anti-money laundering legislation
- Where cash is the normal medium of exchange
- Which have a politically unstable regime with high levels of public or private sector corruption
- Which are known to be drug producing or drug transit countries or
- Which have been classified as countries with inadequacies in their anti-money laundering regulations

The National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organisations Committee UAE (NAMLCFTC) is responsible for preparing and developing a national strategy to combat crime and proposing related regulations, policies, and procedures in coordination with the competent authorities, and monitoring their implementation. The NAMLCFTC represents the UAE in international forums related to Money laundering. The NAMLCFTC, as per the directives of the Financial Action Task Force (FATF)[4] classifies as 'High Risk' jurisdictions having significant strategic deficiencies in their regimes to counter money laundering, terrorist financing and proliferation financing. These are to be accessed through the NAMLCFTC web page: https://www.namlcftc.gov.ae/en/high-risk-countries.php.

[4]The Financial Action Task Force ('FATF') is an intergovernmental body responsible for developing and promoting policies to combat money laundering and terrorist financing. Internationally, FATF has done much to encourage governments to adopt minimum standards including making their national regulators require financial services firms in their jurisdictions to follow specific client due diligence procedures to combat money laundering and terrorist financing.

NAMLCFTC listed High Risk Countries, categorized into on both "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring" should be treated as 'Countries with Elevated Risk' along with any FATF defined Non-Cooperative Countries and Territories (NCCTs). All staff are required to perform EDD and refer any client in a country with elevated risk to the MLRO before any transaction for the client is considered/enacted by the Firm.

Note: It is obligatory for the company to report any transactions involving natural persons or legal entities from'high-risk jurisdictions subject to call for action' before conducting such transaction. Such reported transactions may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.

For High-Risk Clients, additional due diligence measures (i.e. Enhanced Due Diligence - EDD) are requiredwhich will involve identifying any issues that may pose a risk to the company. This process will involve reviewing any existing KYC and CDD information, the professional reputation, person and corporate history, ownership and control including Beneficial Owners, Ultimate Beneficial Owner, directors, shareholders or certain related parties, reputation, political links and associations, standing with law enforcement, criminal links and associations and any other relevant factors. Where the Client has a complex organizational structure, EDD should be undertaken to heighten the company's understanding of the client's corporate/ownership structure and the chain of command. Further guidance on EDD is covered in section 4.5 of this Manual.

4.2 Due Diligence Process

The company must undertake due diligence measures either prior to or during the establishment of a business relationship or the opening of an account, or prior to the execution of a transaction for a customer with whom there is no business relationship. As a rule exceptions should not be promoted, any exceptions to the rule should be discussed and approved only by the Compliance Officer in line with the Guidance for DNFBP 2019 (Part III Section 6.2).

Identification and ID verification of customers is a fundamental component of the KYC/CDD process. Core components of identification are:

- Personal data including details such as the name, identification number, nationality, date and place of birth or date and place of establishment, in the case of a legal person
- Principal address, including evidence of the permanent residential address of a natural person, or the registered address of a legal person. Types of address verification that may generally be considered acceptable include, but are not limited to
    - Bills or account statements from public utilities, including electricity, water, gas, ortelephone line providers
    - Local and national government-issued documents, including municipal tax records
    - Registered property purchase, lease, or rental agreements
    - Documents from supervised financial institutions, such as bank statements or insurancepolicies
- Verify the identity of the client and Ultimate Beneficial Owner, Beneficial Owner, beneficiaries, or controlling persons on the basis of original or properly certified documents, data or information issued by or obtained from a reliable and independent source. Adopting a risk-based approach to CDD, the company should obtain, verify, and record the following identification information:
    - Full business name and any trading name;
    - Registered or business address;
    - Copy of the certificate of incorporation/ Certificate of Registration reflecting the date ofincorporation or registration, place of incorporation or registration
    - A valid commercial or professional license/ Trade License Including the renewal date

- Copy of the articles of association or statutes
- TAX Identification Card/ Certificate reflecting the TAX Number for the entity
- Latest annual report audited and published (where available & applicable)
- The identity of the directors, partners, trustees, or equivalent Persons with executive authority of the legal person
- Identify and verify the Beneficial Owners by looking through each layer of legal persons or Legal Arrangements with interests/stake of 10% or more and until the natural personswith owning or controlling interests as the Ultimate Beneficial Owner with 25% or morein aggregate are identified

For a trust, a certified copy of the trust deed to ascertain the nature and purpose of the trust anddocumentary evidence of the appointment of the current trustees.

- The following documentary evidence must be obtained as a minimum to verify a corporate or financial institution's identity
- For regulated entities, a copy of the extract of the register of the regulator. This cannormally be found on the regulator's website
- For listed companies, a copy of the extract of the exchange's website
- For state-owned companies, a copy of the state law or edict creating the entity

- For identification and verification of foreign nationals, whether customers or Beneficial Owners, Ultimate Beneficial Owner, beneficiaries or controlling persons, documents that are legally valid in the relevant jurisdictions should only be taken. These could be validated through
  - Contacting the relevant foreign embassy or consulate, or the relevant issuing authority;
  - Using commercially available applications to validate the information in machine-readable zones (MRZs) or biometric data chips of foreign identification documents.
- Identity of any person legally empowered to act or transact business on behalf of the customer inaddition to the customer, Beneficial Owners, Ultimate Beneficial Owner, beneficiaries, and controlling persons has to be verified. Such persons include
  - Signatories, or other persons with authorized remote access to an account, such asinternet or phone banking users;
  - Parents or legal guardians of a minor child, or legal guardians of a physically or mentallydisabled or incapacitated person
  - Attorneys or other legal representatives, including liquidators or official receivers of alegal person or arrangement.
- For verifying the authority of the person purporting to act on behalf of a customer the followingdocuments should be checked
  - A legally valid power-of-attorney
  - A properly executed resolution of a legal person's or legal arrangement's governing board or committee
  - A document from an official registry or other official source, evidencing ownership or the person's status as an authorized legal representative
  - A court order or other official decision
- Identify and assess any potentially adverse information
- Understand the Client's Source of Funds
- Understand the Client's Source of Wealth (transaction not commensurate to the client profile)

4.3 CDD for legal entities (e.g. corporates, establishments, LLC etc.)

Adopting a risk-based approach to CDD, firm should obtain, verify, and record the following identificationinformation:

- Full business name and any trading name
- Registered or business address
- Copy of the certificate of incorporation/ Certificate of Registration reflecting the date of incorporation or registration, place of incorporation or registration
- A valid commercial or professional license/ Trade License Including the renewal date
- Copy of the articles of association or statutes
- TAX Identification Card/ Certificate reflecting the TAX Number for the Entity
- Latest annual report audited and published (where available & applicable)

- The identity of the directors, partners, BO's, UBO's, trustees or equivalent Persons with executiveauthority of the legal Person
- For a trust, a certified copy of the trust deed to ascertain the nature and purpose of the trust anddocumentary evidence of the appointment of the current trustees.

The following documentary evidence must be obtained as a minimum to verify a corporate or financial institution's identity:

- For regulated entities, a copy of the extract of the register of the regulator. This can normally be found on the regulator's website
- For listed companies, a copy of the extract of the exchange's website
- For state-owned companies, a copy of the state law or edict creating the entity

4.4 Simplified Due Diligence (SDD)

SDD, as a result of a risk-based assessment, may involve more lenient application of the due diligence requirements

- Verifying the identity of the client and the Ultimate Beneficial Owner, after the establishment ofthe business relationship; authentication of documents may not be necessary and could be limited to a copy being provided
- Less detailed inquiries on the purpose of the business relationship being established, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions
- Limited supervision of the business relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information
- Limited enquiry of the client's Source of Funds or Source of Wealth

If the company decides on the above, it must be documented accordingly. Any modification to the CDD requirements must be proportionate to the Client's money laundering risks. Therefore, firm will not apply simplified CDD measures to a Client, beneficiary, or business relationship when there is a suspicion of money laundering and/or terrorist financing.

4.5 Enhanced Due Diligence (EDD)

Where Clients are assessed as having a high-Risk Rating, the company is required to undertake enhanced CDD. As a result, it should consider:

- Increased scrutiny and higher standards if verification and documentation from reliable and independent sources with regards to the customer's identity/profile. Obtaining and verifying additional:
    - Identification information on the Client and the Ultimate Beneficial Owners and all Beneficial Owner (shareholding of >10%)
    - Information on the intended nature of the business relationship
    - Information on the reasons for a Transaction
- Updating more regularly the CDD information which it holds on the client and any Beneficial Owners, Ultimate Beneficial Owner
- Detailed inquiry and evaluation of reasonableness with regards to the purpose of the business relationship/nature of business and verify and corroborate information on:
    - The Client's Source of Funds
    - The Client's Source of Wealth
- Increasing the degree and nature of monitoring of the business relationship and Client's Transactions or activities along with additional controls (transaction limits) if/as required in discussion with compliance and senior management
- Annual and/or trigger (as a fall out of any red flags) review of the client profile and due diligenceinformation
- Obtaining the rationale behind the transactions executed or expected to be executed
- Requiring that the initial transaction is carried out through an account opened in the client's name with a credit from a financial institution subject to the AML rules or regulated in a FATF country (i.e. not from a country with elevated risk)
- Obtaining the approval of senior management, to commence a business relationship with a Client
    - As a general rule, any client that has been categorized as having a high risk it is expected that the ultimate Beneficial Owners of the major shareholders (>10%) wouldbe identified and screened.

4.6 Ongoing Monitoring

Ongoing supervision of customers' activity, including auditing transactions executed throughout the course of the relationship to ensure that they are consistent with the information, types of activity, and risk profiles of the customers is necessary control highlight any gaps/red flags. The risk category of the client would be the driver for the frequency of ongoing monitoring.

- Monitor Transactions undertaken during the course of its client relationship to ensure that the Transactions are consistent with firm's knowledge of the client, his business and risk rating
- Pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose. Also enquire intothe background and purpose of these transactions
- Periodically review the adequacy of the CDD information it holds on clients and Beneficial

Owners, Ultimate Beneficial Owner, to ensure that the information is kept up-to-date, particularly for Clients with a high-risk rating

- Periodically review each client to ensure that the risk rating assigned to a client remains appropriate for the client in light of the money laundering risks

Methods that may be considered for the purposes of ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined
- Transaction-based rules, in which a certain percentage (or even all) of the transactions of acertain type are examined
- Location-based rules, in which a certain percentage (or even all) of the transactions involving aspecific location (either as origin or destination) are examined
- Customer-based rules, in which a certain percentage (or even all) of the transactions of particular customers are examined

4.7 Periodic Review

In some situations (in the case of ongoing business relationships with suppliers or customers) the company may be in a position to monitor the status and activity of the business relationship over time. However, in other situations (such as those involving occasional or one-off customer transactions, or retail sales), it may not always be possible for the firm to perform detailed ongoing monitoring of the entirety of their business partners' or customers' activity. Nevertheless, it is important that the firm take reasonable steps to protect themselves from misuse by criminals and terrorists. Particularly in circumstances in which high-risk customers have been identified,

As a general rule a periodic review of the client's overall profile should be considered in line with their risk profile.

- Low risk MLRR (Money Laundering Regulation Review) every 3 years
- Medium risk MLRR every 2 years
- High risk MLRR or any clients that carry PEP risk (i.e. companies with PEPs as directors or Beneficial Owners or Ultimate Beneficial Owner) on at least yearly basis

The company should also undertake periodic reviews to ensure that non-static client identity documentation is accurate and up to date. Examples of non-static identity documentation include passport number and residential/business address and, for corporates/financial institutions (i.e. legal persons), its share register or list of directors. The company has designed a spreadsheet listing all clients and what information it holds per client.

Note: Ongoing Monitoring and Periodic Review

The company continues to undertake appropriate due diligence under section 4.6 & 4.7 above after establishing a business relationship with a customer. The Compliance Officer would be responsible to ensure that a detailed MIS (Management Information System) reflects customer wise, product wise, transaction mode (cash/non-cash), risk category wise, and that quarterly, bi-annual and annual sales reports are generated from the system for analysis and highlight any concerns based on trends or red flags. Once the base data is analyzed the CO/MLRO would narrow

down on relationships which may be reviewed as part of Ongoing Monitoring and Periodic Review.

4.8 Sources of information

Where a copy of an original identification document is made by the company, the copy should be dated, signed, named and marked with 'original sighted'. It may not always be possible to obtain original documents in office. Where identification documents cannot be obtained in original form, the company should obtain a copy certified as a true copy by a person of good standing such as a:

(a) Another Employee of firm who has seen the originals

(b) Registered lawyer or notary

(c) Chartered accountant

(d) Bank manager

(e) Police officer

(f) Employee of the Person's embassy or consulate, or

(g) Similar Person

Downloading publicly available information from an official source (such as a regulator's or other official government website) is sufficient to satisfy the CDD requirements. The regulator also considers that CDDinformation and research obtained from a reputable company or information-reporting agency may alsobe acceptable as a reliable and independent source as would banking references and, on a risk-sensitive basis, information obtained from researching reliable and independent public information found on the internet or on commercial databases.

The company should be proactive in obtaining and making appropriate use of available national and internationalinformation on money laundering or terrorist financing. This includes information such as suspect lists ordatabases from credible public or private sources (Global Risk Profile to be used). It is recommended to periodically perform checks of names appearing on these lists against their own Client databases and records and to monitor transactions accordingly. Any evidence that has been obtained in a foreign language must be translated into English.

4.9 Reliance on a third party to conduct CDD

While CDD by third party is allowed the procedures for determining the adequacy of a third party's CDD measures should be defined in advance, including the evaluation of such factors as the comprehensiveness and quality of its policies, procedures, and controls; the number of personnel dedicated to customer due diligence; and its audit and/or quality assurance policies in regard to CDD. Periodic assessment of the effectiveness should be undertaken.

Some examples of the third parties the firm may rely on to conduct one or more elements of CDD on its behalf:

- A law firm, notary, or other independent legal business, accounting firm or audit firm in anotherjurisdiction
- A financial institution

The company may also rely on the information previously obtained by a third party which covers one or more elements of CDD.

Where the company relies on a third party listed above, it may only do so if and to the extent that:

- It immediately obtains the necessary CDD information from the third party
- It takes adequate steps to satisfy itself that certified copies of the documents used to undertakethe relevant elements of CDD will be available from the third party on request without delay
- The third party noted above is subject to regulation, including AML, by a financial services regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF recommendations and it is supervised for compliance with such regulations
- The third party noted above has not relied on any exception from the requirement to conduct any relevant elements of CDD which firm seeks to rely on
- The information is up to date

If the company is not reasonably satisfied with the CDD undertaken by a third party, it must perform the CDD itself with respect to any deficiencies identified. Notwithstanding reliance on a third party, it should be noted that the company remains responsible for compliance with, and liable for any failure to meet, the CDD requirements in this module.

Reliance on third party KYC will all be noted by the company on the client onboarding form, as will any deficiencies noted, and steps taken to overcome these.

4.10 Onboarding

The company's manager is responsible for populating and completing the client onboarding form with relevant client information which will evidence that all necessary and appropriate enquires were made accordingly. The client onboarding form must not be given to the prospective client to complete, and they are not required to sign the form. The client onboarding form will be signed by the company's employee. The employee must provide the client onboarding form and supporting KYC documentation to the Senior Management and Compliance Officer for review and approval signatures. Records must be maintained of decisions taken regarding client onboarding.

Each categorization will be evaluated to provide the overall Client Risk Assessment Rating (CRAR). The overall CRAR should be noted in the client onboarding form. Further guidance on the various factors from which the CRAR is calculated is provided in Appendix 3 of this Procedures Manual. The CRAR will determine the appropriate level of due diligence to be performed.

Prospective Clients who do not meet the requirements for normal levels of CDD will be subject to more rigorous review which may include enhanced CDD. The level of enhanced CDD will be assessed by the Compliance Officer, in order to aid business decisions and protect the company's commercial reputation. The aim of enhanced CDD is, in essence, to provide the company with an understanding of the exact nature of the risks associated with an entity or individuals, thereby allowing firm to make risk-sensitive commercial decisions.

The populated client onboarding form must be signed by the company manager/ employee and sent to the Compliance Officer, together with all relevant CDD supporting documentation, for

review and performance of name screening using Global Risk Profile. The Compliance Officer will then review the documentation to ascertain whether sufficient information is known to verify the proposed client and also to check the client classification, confirm whether the proposed client is a prescribed as a low risk customer, assess the CRAR, confirm whether further due diligence or documentation is required and generally to review that the client onboarding form has been populated.

CHAPTER 5: INTERNAL AND EXTERNAL REPORTING REQUIREMENTS

5.1 Internal reporting requirements

If an employee either, knows or suspects or has reasonable grounds for knowing or suspecting that the attempted transaction or funds involved (in whole or part) are a) Proceeds of Crime, b) Related to the crimes or money laundering and financing of terrorism or c) Are being intended to be used in such activity, then the employee is obliged to make an internal Suspicious Activity Report ('SAR') to the Compliance Officer, using the template in Appendix 5 for internal review. Such an obligation is still applicable even if no business relationship was developed at that point in time due to the suspicion aroused.

Whether or not an employee consults with his line manager or other employees, the obligation remains with the individual staff member to notify the Compliance Officer on the suspicion based on reasonable grounds.

Disciplinary action can be taken against any employee who fails to make a report. Senior management and employees are reminded that failure to report suspicions of money laundering may constitute a criminal offence that is punishable under the laws of the UAE.

5.2 Identification of Suspicious Transactions

All staff should note that the presence of an indicator of suspicion does not necessarily always mean that a transaction is suspicious and needs to be reported. When determining whether a transaction is suspicious, due consideration should be given to the nature of the specific circumstances, including the products or services involved, and the details of the customer in the context of its due diligence profile. In some cases, patterns of activity or behavior that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another.

The idea of 'reasonable grounds to suspect introduces an objective rather than a subjective test of suspicion by assessing whether or not suspicion was ignored by way of:

- Willful blindness
- Negligence that is willfully and recklessly failing to make the adequate enquiries; or
- Failing to assess adequately the facts and information that are either presented or available.

ML/FT Typologies

Some common methods/typologies used by criminals for the purposes of ML/FT involved in the company's business/field/sector are stated below. These methods broadly align with the classical stages of the ML/FT process (i.e. placement, layering, and integration)

- **Use of precious metals (PMs) and gold as an alternative to currency**. Due to their specific characteristics, diamonds and gold, in particular, can be an attractive means to store value. This status can lend itself to the utilisation of PMs by criminals as an alternative form of payment for illicit goods and services, which can be smuggled relatively easily and later converted to cash or other traditional and non-traditional forms of value orvalue transfer, bypassing the formal financial sector and its associated controls. Analysis of case studies has shown a correlation between the use of diamonds and gold as currency and drug trafficking; however, it has also been reported in cases related to other categories of crime, such as illegal arms dealing, human trafficking, environmental crimes, and others.
- **PMs as stored value instruments/means to realise the proceeds of crime.** Diamonds and gold, in particular, are an international commodity, easily traded, transferable across borders, and able to retain (or even appreciate in) value over relatively long periods of time. These characteristics, along with their relative anonymity, and even their ability to be insured, warehoused, and changed into different physical forms, make them well-suited to serve as a means of longer-term value storage and ML.
- **Laundering illegal PMs and/or the use of PMs to launder the proceeds of crime.** The PMs supply chain is complex and can involve multiple participants in each stage, with varying levels of control and numerous vulnerabilities to ML/FT and associated predicate offences. Criminals may utilise a variety of techniques to realise value from illegal PMs, or to conceal, disguise, and/or transfer the proceeds of crime by utilising financial flows associated with the trade in PMs, at different stages of the supply chain. Such techniques may include but are not limited to: theft or embezzlement; smuggling; commingling of illicit and legal materials; forgery or fraudulent certification; transfer pricing; misrepresentation of quantity, quality, or type of PMs; and many others. These techniques are often used when laundering the proceeds of crime through wholesale or retail trading.
- **Trade-based ML.** Due to the global nature of the trade in PMs, criminals may exploit opportunities to utilise this typology through PMs-related transactions and related financial flows. Some of the techniques employed include but are not limited to: over-invoicing, under-invoicing, or fraudulent invoicing, customs/VAT fraud, forgery and falsification of documentation, virtual trading, and others.These techniques are often associated with the use of major trading hubs for PMs, including free trade zones.
- **Physical smuggling of PMs.** Due to their high value-to-weight ratio, and other characteristics of PMSthat make them difficult to detect or trace, they can be smuggled fairly easily. This is often done in conjunction with the other ML/FT methods referred to above, and may involve a number of differenttechniques, including the disguising of certain types of PMs as common low-value objects.

Key to recognizing what is suspicious is knowing enough about the client profile and the client's normal pattern of activities/transactions in order to recognize when a transaction is abnormal. Circumstances that might give rise to suspicion or reasonable grounds for suspicion may be:

- <u>The Business Relationship, Counterparty, or Customer:</u>
- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, or the company has reasonable doubt that the provided information is correct or sufficient
- Is reluctant, unable, or refuses to explain:

- their business activities and corporate history;
- the identity of the beneficial owner;
- their source of wealth/funds;
- why they are conducting their activities in a certain manner;
- who they are transacting with;
- the nature of their business dealings with third parties (particularly third parties locatedin foreign jurisdictions).

- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources
- Is a designated person or organisation (i.e. is on a Sanctions List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, withoutsufficient justification.
- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person or has familial or professional associations with a person who ispolitically exposed.
- Is a foreign national with no significant dealings in the country, and no clear economic or otherrationale for doing business with the company.
- Is located a significant geographic distance away from the company, with no logical rationale.
- Refuses to co-operate or provide information, data, and documents usually required to facilitatea transaction, or is unfamiliar with the details of the requested transaction.
- Makes unusual requests (including those related to secrecy) of the company or its employees.
- Is prepared to pay substantially higher fees than usual, without legitimate reason.
- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services (for example, smelting and reshaping of gold into ordinary-looking items, or re-cutting and polishing precious stones) that could improperly disguise the nature of the PMs or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.
- Claims to be a legitimate company, business, or entity, but cannot demonstrate a history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such asLinkedIn or others).
- Is registered under a name that does not indicate that activity of the company is related to PMs,or that indicates activities different from those it claims to perform.
- Is a business that uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot

be located on internet mapping services (such as Google Maps).

- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised the transaction.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering, terrorism financing, or corruption risk.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Appears to be acting according to instructions of unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Requests payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or installment arrangements, or payment in several different forms), or which involve third parties.
- Provides identification, records or documentation which appear to be falsified or forged.
- Requires that transactions be effected exclusively or mainly through the use of cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or other such payment methods), or through virtual currencies, for the purpose of preserving their anonymity, without adequate and reasonable explanation.

The Transactions:

- Involves the use of a large sum of cash, without an adequate explanation as to its source orpurpose.
- Involves the frequent trading of PMs (especially diamonds and gold) or jewellery for cash in smallincremental amounts.
- Involves the barter or exchange of PMs (especially diamonds and gold) or jewellery for otherhigh-end jewellery.
- Appears structured so as to avoid the cash reporting threshold.
- Involves delivery instructions that appear to be unnecessarily complex or confusing, or which involve foreign jurisdictions with no apparent legitimate connection to the counterparty or customer.
- Includes contractual agreements with terms that are unusual or that do not make business sensefor the parties involved.
- Involves payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves PMs with characteristics that are unusual or do not conform to market standards.
- Involves the unexplained use of powers-of-attorney or similar arrangements to transact businesson behalf of a third party.
- Appears to be directed by someone (other than a formal legal representative) who is not a

formalparty to the transaction.

- Involves a person acting in the capacity of a director, signatory, or other authorised representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries (countries with elevated risk), when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involves several successive transactions which appear to be linked, or which involve the sameparties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared tothe assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreignnationals, who may or may not be resident for tax purposes.
- Involves unexplained last-minute changes involving the identity of the parties (e.g. it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.
- Involves circumstances in which the parties:
    - Do not show particular interest in the details of the transaction
    - Do not seem particularly interested in obtaining a better price for the transaction or inimproving the payment terms
    - Insist on an unusually quick completion, without a reasonable explanation.
- Takes place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.
- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves indications that the counterparty does not have or does not wish to obtain necessary governmental approvals, filings, licenses, or other official requirements.
- Involves any attempt by a physical person or the controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to: over- or under-invoicing of goods or services, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under-shipments (e.g. false entries on bills of lading); or multiple trading of the same goods and services).

<u>The Means of Payment:</u>

- Involves cash, cash equivalents (such as cashier’s cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or similar instruments), negotiable bearer

instruments, or virtual currencies, which do not state the true payer, especially where the amount of such instruments is significant in relation to the total value of the transaction, or where the payment instrument is used in a non-standard manner.

- Involves unusual deposits (e.g. use of cash or negotiable instruments, such as traveler's cheques, cashier's cheques and money orders) in round denominations (to keep below the reporting

  threshold limit) to pay for PMs. The negotiable instruments may be sequentially numbered orpurchased at multiple locations and may frequently lack payee information.
- Is divided into smaller parts or installments with a short interval between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves third-party payments with no apparent connection or legitimate explanation.
- Cannot be reasonably identified with a legitimate source of funds.

A transaction that appears unusual is not necessarily suspicious. Even clients with a stable and predictable transaction profile will have periodic dealings that are unusual for them. Many clients will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises. If an employee is in doubt, they must consult the Compliance Officer for guidance.

5.3 Compliance Officer obligations

If the Compliance Officer receives an internal SAR or STR, they must without delay:

- Review the documents the circumstances in relation to which the notification was made
- Determine whether in accordance with Federal AML legislation a Suspicious Activity Report or a Suspicious Transaction Report must be made to the Competent Authority (using the template in Appendix 6) and document such determination
- If required, makes a SAR/STR to the Competent Authority as soon as practicable
- Notify the Federal Authority of the making of such SAR/STR immediately following its submissionto the Competent Authority and follow up on advised actions if any
- Keep the firm's Senior Management informed

The Compliance Officer must document:

- The steps taken to investigate the circumstances in relation to which an internal SAR/STR is made
- Where no external SAR/STR is made to the competent authority, justification on the rationale whyand how the risk was negated or mitigated

5.4 External reporting requirements

Making an external SAR/STR to the Competent Authority and notifying is the sole responsibility of the Compliance Officer. It is the compliance officers' decision to make independently and is not subject to the consent or approval of any other person. In this regard, the Financial Intelligence Unit (FIU) has established an online Suspicious Transaction & Suspicious Activity Reporting System,

which requires the compliance officer to choose from a list of suspicious indicators when filing a suspicious transaction report(STR).

The template as shared under GoAML for external SAR and STR is required to be used to report external SARs to the Competent Authority by the Compliance Officer and Update GoAML, web-portal for externalSAR

All sections of the external SAR/STR must be completed fully. SARs/STRs should also include the following:

- All information that supports the SAR/STR
- Any additional information which would help the Competent Authority / FIU to further itsinvestigations
- Any additional information which could link the SAR/STR to other SARs/STRs and otherinvestigations

5.5 Best practice when completing SAR/STR

When completing the external SAR/STR template, the following guidance may be helpful. However it is recommended that the CO MLRO reviews the detailed video on How to file SARs/STRs (Appendix 6).

- Full Name of the Customer (or potential) < Clearly identify client name in full >
- Passport number / Details of License <Always input some identification details, if unknown explain why>
- Nationality <If official nationality is unknown at least provide an indication e.g. Middle Eastern.>
- Address/ known addresses <All and any contact details of the suspected individual.>
- Amount of suspected transaction <This is the amount of currency that you suspect is involved in the transaction. If no transaction took place and it was a suspicious activity only then insert nil (with description of the actual suspicion). However, in some cases of suspicious activity money isdiscussed in this case the amount needs to be included.>
- Source of Suspicion <Clearly identify the reason for suspicion e.g. Suspicious source of fund, any information gathered during the conversation etc.>
- Date <Date of submission>

The Compliance Officer should consider the following "Do's and Don'ts" when submitting an SAR/STR:DO:

- Do submit all supporting documentation with your SAR/STR
- Do submit a SAR for suspicious behavior/activity or an attempted transaction only i.e. notransaction is required while for STR it should be based on a suspicious transaction
- Do submit an SAR/STR within a reasonable timeframe of identified suspicious
- Do include all relevant details in your SAR/STR including source of funds, linked accounts, etc.
- Do report confidentially without involving unrelated people as it could alert the customer and beconsidered as "Tipping Off"
- Do maintain your SARs/STRs as per the record keeping requirements
- Do send additional SARs/STRs when further information comes to light in order to

supplementthe original suspicion; Please ensure that you make references to previous submissions

- Do provide your contact details so that the competent authority can contact you with follow upquestions
- Do provide a clear trail of your cause for suspicions and as much detail as possible about theperson(s) involved. Do notify of any SAR/STR you have lodged with the competent authority

DO NOT

- Do not terminate the relationship intentionally prior or post raising the STR unless there is a logical and/or unavoidable reason behind such action. Please wait for an official response from the Competent Authority / FIU.
- Do not insert "refer to documents attached" under "Source of Suspicion." A brief explanation in the space provided is required and identify the suspicion clearly and concisely. Do not forget to notify when you have lodged an SAR/STR with the Competent Authority.

The Compliance Officer has to complete the submission of the external SAR/STR, under UAE Federal LawAML Legislation through the GoAML portal.

Information contained in an SAR/STR is confidential. The company is protected from any criminal, civil or administrative liability which may result from providing the required information in an SAR/STR which has been submitted in good faith.

5.6 FIU

The FIU (**Financial Intelligence Unit)** is established within the premises of the Central Bank, and it operates independently by legal and regulatory mandate as the central national agency with sole responsibility for performing the following functions. The following are being shared here to help the team understand what the FIU does and the relevant touch points with respect to the firm:

- Receiving and analysing Suspicious Transactions Reports and disseminating the results of its analysis to the Competent Authorities of the State
- Receiving and analysing reports of suspicious cases from the Federal Customs Authority
- Requesting additional information and documents relating to STRs, or any other data or information it deems necessary to perform its duties, from FIs, DNFBPs, and Competent Authorities, including information relating to customs disclosures
- Cooperating and coordinating with Supervisory Authorities by disseminating the outcomes of itsanalysis, specifically with respect to the quality of STRs, to ensure the compliance of FIs and DNFBPs with their statutory AML/CFT obligations
- Sending data relating to STRs and the outcomes of its analyses and other relevant data, including information obtained from foreign FIUs, to national Law Enforcement Authorities, prosecutorial authorities and judiciary authorities when actions are required by those authorities in relation to a suspected crime
- Exchanging information with its counterparts in other countries, with respect to STRs or any otherinformation to which it has access.

5.7. Post SAR/STR filing(with FIU) process

Following the reporting of the SAR/STR with the FIU the following actions needs to be taken:

- Await for and follow instructions from the FIU
- Maintain strict confidentiality of the FIU instructions received
- Classify the client on whom the SAR/STR has been reported as 'High Risk'
- Report any additional suspicious, adverse information on the same client with the FIU
- While FIU reviews the SAR/STR submitted & awaiting their decision, overmanage and delay theclient transactions as much as possible and ensure that the client is not tipped off
    - o Due to the delay in processing the transaction if the client may withdraw/cancel the transaction, the compliance officer should reach out to FIU informing of the same and seek the next steps within a reasonable time period while keep the client waiting on somepretext. In the event the compliance officer does not receive instructions post the aboveescalation, the firm is well within its right to cancel the transaction and exit the client.

5.8 Tipping off

The company's Compliance Officer is obliged to maintain confidentiality with regard to both the information being reported in the SAR/STR and to the act of reporting itself.

It is a federal crime for the firm, or their managers, employees or representatives, to inform the customer/client or any other person, whether directly or indirectly, that a SAR/STR report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction of the client.

Appendix:

APPENDIX 1: COMPLIANCE MANUAL & AML PROCEDURES CERTIFICATION

To,
The Compliance Officer,
AETERNO FZE
SAIF Zone, Sharjah, UAE

I confirm receipt of Aeterno Compliance and Anti-Money Laundering Procedures Manual. I am either aware of location of Compliance AML Manual should I need to access it or agree I will keep the Manual for further reference. I confirm that I have understood Procedures of Compliance AML Manual and accept that the requirements setout within it form part of my contract of employment.

I hereby undertake to:

- To act and conduct myself in compliance with AML rules and regulations, as stipulated within:
  - Decree Federal law No. (20) of 2018 on Anti-Money Laundering and combating the financing of terrorism and illegal organizations.
  - Cabinet Decision No. (10) of 2019 Concerning the implementing regulation of Decree Federal lawNo. (20) of 2018 on Anti-Money Laundering and combating the financing of terrorism and illegal organizations.
- Agree to adhere to the spirit as well as the letter of the rules and regulations.
- I will observe and comply with all of the Firm's requirements on AML/CDD that may be amended from time to time.
- I have and will continue to act and conduct in line with this manual, UAE rules and regulations and when in doubt, I will discuss with MLRO as to the specific rules.

I understand, acknowledge and agree that:

- all provisions of Aeterno Compliance AML Manual apply to me.
- failure to comply with the requirements, rules and/or regulations may have serious consequences for AETERNO FZE and its employees.
- any breaches may result disciplinary actions including termination of employment.
- I have read and understood all the provisions in the Compliance AML Manual and agree to abide by and accept the policies and procedures contained herein.

By signing this certification, I hereby acknowledge that

☐ I am a new employee and accept that the requirements set out in Aeterno Compliance AML manual form a part of my employment contract.

Employee Name: **Date:**

Employee Signature:

APPENDIX 2: COMPLIANCE MANUAL & AML PROCEDURES ANNUAL CERTIFICATION

To,
The Compliance Officer,
AETERNO FZE
SAIF Zone, Sharjah, UAE

I confirm to have reread and understood Aeterno Compliance and Anti-Money Laundering Procedures Manual. I am aware of location of Compliance AML Manual should I need to access it or agree I will keep the Manual for further reference. I confirm that I have understood Procedures of Compliance AML Manual and accept that the requirements setout within it form part of my contract of employment.

I hereby undertake to:

- To act and conduct myself in compliance with AML rules and regulations, as stipulated within:
  - Decree Federal law No. (20) of 2018 on Anti-Money Laundering and combating the financing of terrorism and illegal organizations.
  - Cabinet Decision No. (10) of 2019 Concerning the implementing regulation of Decree Federal lawNo. (20) of 2018 on Anti-Money Laundering and combating the financing of terrorism and illegal organizations.
- Agree to adhere to the spirit as well as the letter of the rules and regulations.
- I will observe and comply with all of the Firm's requirements on AML/CDD that may be amended from time to time.
- I have and will continue to act and conduct in line with this manual, UAE rules and regulations and when in doubt, I will discuss with MLRO as to the specific rules.

I understand, acknowledge and agree that:

- all provisions of Aeterno Compliance AML Manual apply to me.
- failure to comply with the requirements, rules and/or regulations may have serious consequences for AETERNO FZE and its employees.
- any breaches may result disciplinary actions including termination of employment.
- I have read and understood all the provisions in the Compliance AML Manual and agree to abide by and accept the policies and procedures contained herein.

By signing this certification, I hereby acknowledge that

☐ Annual Certification - I have at all times, and will continue to be, in compliance with both the spirit and the specific requirements of all of the provisions of the Firm's Compliance Manual.

Employee Name: **Date:**

Employee Signature:

APPENDIX 3: CLIENT RISK ASSESSMENT RATING (CRAR)

The Client Risk Rating depends on the assessment across the 'Risk Factors' as a part of the Risk Based Approach. The risk factors applicable to (insert client name) and their line of business have been duly considered and defined along with adequate weightages in the Risk Based Approach Grid (excel file circulated separately).

Once the required information is obtained from the client and input the 'aggregate risk' of all the factors is taken into consideration to form the overall Client Risk Assessment Rating of the client known as the CRAR, with clients listed as

i. Low
ii. Medium
iii. High

APPENDIX 4: CLIENT ONBOARDING FORMS (attached separately)

CLIENT CDD - Details to be filled by the Staff (Refer to Aeterno CDD Process Note for detailed procedure)

Name of Client: _____

SECTION 1

CLIENT SCREENING: *(To be completed by Designated Screening Staff; Add rows as needed)*

Customer Screening – Name as per Passport *(Include entities and all associated individuals in the relationship)*	**Screening date**	**Result: (No match / PEP / Other)**	**Remarks for Hits**
List of Directors – Name as per Passport	**Screening date**	**Result: (No match / PEP / Other)**	**Remarks for Hits**
List of shareholders/ultimate beneficial owners	**Screening date:**	**Result: (No match / PEP / Other)**	

Source of Funds (SOF) Information Sheet

Entity Details

Company name				
Industry				
Period of ownership				
Annual Revenues				
Annual Profits				
% of ownership				
Country				
Nature of business				

Source of Funds

Guidance for filling SOF Section: • History of business • Details of various companies that the client is associated with, if any • % of business ownership • Annual income from the business • Details of the business valuation. • Information on sale of business if any. • Any link with sanctioned countries (buyers / suppliers) • % business from high risk business. • Corroborative evidence as required by Compliance / AML manual requirements. • Provide similar information for all UBO's

SECTION 2

CALCULATION OF AML RISK *(To be completed by Compliance)*

Applicability	Risk Factors	Score	Risk Tagging
	High Risk Country	3	HRC
	HRB (other factors not listed elsewhere in this list)	3	HRB (O)
	Complex structure (3 or more additional layers excluding the UBO)	6	CPX
	Non-FATF trustees and individual trustees	6	NFT
	Charitable trusts and waqfs	6	CTW
	Bearer Share company (including Companies which have the ability to issue bearer shares)	6	BSA
	Walk in client / non-face-to-face business relationships or transactions	6	WIC
	Nominee Shareholder and / or Nominee directors	6	NSD
	PEPs	12	PEP
	Sanctions Risk	12	SAN
	HRB (Weapons)	12	HRB (W)
	HRB (Casino / Gambling / Cash intensive)	12	HRB (C/G)
	Clients from jurisdictions having AML deficiencies	12	HRC (D)
	Reputationally Exposed Person	12	REP
	High Tax Risk	12	HTR
	SAR filed against the client	12	SAR
	Total Risk Calculation		

AML Risk Score Guide:

Composite Score	Resultant AML Risk Rating	Periodic Review
Below 6	Low Risk - Simplified due diligence required	3 years or earlier on triggering event.
6 to 11	Medium Risk - Standard due diligence required	2 years or earlier on triggering event.
12 and above	High Risk - Enhanced due diligence required	1 year or earlier on triggering event.

Risk Scores impacting the account:	
Overall AML Risk:	
Next review date:	

For High-Risk Rating:

High Risk factors identified:	
Brief background about the risks identifie	
Mitigating factors if any	

For PEP and REPs assess the following factors:

Background of PEP and REP risk	
Brief background about the risks identifie	
CPI index of the jurisdiction from which PEP / REP risk arises	
Impact of PEP / REP on the SOW/ SOF/SOI	
Mitigating factors if any	
Justification for accepting PEP	

DOCUMENTATION CHECKLIST FOR ON-BOARDING *(Add rows as needed)*
Account Opening Form & Declarations:

- Account Opening & KYC Questionnaire

Below mentioned declarations need to be printed on client company letter head, filled, signed & stamped.

- Sanctions Undertaking
- Board resolution
- UBO Declaration

- VAT/TAX Declaration
- PEP Declaration
- Source of funds declaration
- Supply Chain details & declaration

COMPANY Document List:

- Company Profile & website
- Certification of Incorporation
- Trade License
- Memorandum and Articles of Association
- List of UBO's / Shareholders
- Details of Beneficial Owners if not mentioned in M&As
- List of Authorized Signatories
- VAT TRN NO & VAT Registration Certificate
- Corporate Tax Registration Certificate
- UAE GOAML registration number (If UAE Company)
- Export / Import code
- Tenancy Contract of office premise
- Company BANK details (Bank name, account number, IBAN, Branch, SWIFT)
- Anti-Money Laundering AML/CFT Policy, Anti Bribery and Corruption Policy document of company.

Ultimate Beneficial Owner (Ownership Status over 5% or more in company):

- Passport Copy (Front & Back)
- National ID Card (Front & Back)
- Visa Copy
- Proof of Residential Address - Utility Bill
- Authorized Representatives of the Company:
- Passport Copy (Front & Back)
- National ID Card (Front & Back)
- Visa Copy
- Proof of Residential Address - Utility Bill

NOTE: There are new KYC rules in UAE effective 01Feb2023 and UAE Gold refineries need to understand the entire supply chain i.e. physical gold starting from point of origin (Gold Mine) till UAE Gold refinery, so the refinery needs to review KYC, complete due diligence and approve each party involved in the transaction starting from the Miner, Exporter to end Buyer. If there are additional actors in the supply chain *(other than miner, exporter, buyer)*, Aeterno refinery is required to conduct proportionate amount of KYC and due diligence on each actor involved in the supply chain.

[A] Kindly explain proposed / anticipated business relationship with Aeterno Refinery:

[B] Miner: below mentioned documents required from your mine source to perform due diligence on the origin of gold and its supply chain.

- Mining license
- Registration and ownership documents (such as certificate of incorporation, share registry, passport copy of beneficial owners)
- Policies and manuals on AML-CFT, bribery and corruption, human rights, environmental, health and safety, labor, community engagement, ethics and business integrity.

[C] Exporter: below mentioned documents of an exporter in the supply chain.

- Registration and ownership documents (such as certificate of incorporation, share registry, passport copy of beneficial owners)
- Export license.

Any other relevant or material matters not previously covered in this form:

SIGNATURES:

Sales Manager	Date	Signature

Approvals:

The account is considered for on boarding based on the information and documentation provided.

Compliance Officer	Date	Remarks (if any) and Signature

SENIOR MANAGEMENT	Date	Remarks (if any) and Signature

APPENDIX 5: INTERNAL SAR/STR NOTIFICATION FORM

NOTE: below format is for internal review, socialization and discussion purposes only. Once the SAR/STR has been filed on the GoAML portal, the same needs to be printed and saved for record purposes.

- Internal SAR/STR Number:
- Name of Client's representative (if any):
- Current or last known address:
- Phone Number:
- Email:
- Client's Business / Occupation:
- Passport / ID Number or Trade License Number:
- Nationality:
- Location of Business / Incorporation:
- Nature and amount of suspected transactions:
- Details of any connected accounts:
- Reason for suspicion:
- Instructions of the Compliance Officer to the Person making the report:

Approvals:

Compliance Officer	Date	Remarks (if any) and Signature

SENIOR MANAGEMENT	Date	Remarks (if any) and Signature

APPENDIX 6: EXTERNAL SAR and STR FORM:

Template as shared under GoAML for external SAR and STR would require to be used (detailed guidance as shared by the Supervisory Authorities through a video should be referred https://www.youtube.com/channel/UChqcRa_X-2nIOSzrZ8rNZVw.

This needs to be done at the online portal of GoAML.

APPENDIX 7: WHAT ARE PRECIOUS METALS AND PRECIOUS STONES (PMS)?

While the definitions of precious metals and precious stones may vary somewhat depending on region, the most generally accepted classifications internationally, based on factors such as quality, intrinsic value, and rarity, consider the precious metals to consist of gold, silver, and the so-called platinoid metals(principally platinum and palladium); and precious stones to consist of diamonds, emeralds, rubies, and sapphire. While not technically gemstones, pearls are often also included in the category of precious stones and are thus included for the purpose of this supplemental guidance. These generally accepted classifications are reflected in the federal legislation of the UAE, which governs the control, stamping and identification of PMS, as well as the import and export requirements concerning raw diamonds under the internationally accepted Kimberley Process Certification Scheme Appendix 7 (a).

Taking into consideration the above, and without prejudice to any pre-existing or subsequent definitionsincluded in any federal law or regulation of the UAE, the definitions of precious metals and precious stones for the purpose of this supplemental guidance include, but are not limited to, those materials falling under the following categories: Appendix 7 (b)

Precious Metals

- Gold, with a minimum purity of 500 parts per 1,000;
- Silver, with a minimum purity of 800 parts per 1,000;
- Platinum, with a minimum purity of 850 parts per 1,000;
- Palladium, with a minimum purity of 500 parts per 1,000.

Precious Stones

- Diamonds (rough) of any weight in carats;
- Diamonds (polished), with a minimum weight of 0.3 carats per stone if loose, or a minimum weight of 0.5 carats per any single stone mounted in a setting (whether of one or more stones);
- Colored Gemstones (polished Emeralds, Rubies, Sapphires), with a minimum weight of 1 carat per stone if loose, or a minimum weight of 2 carats per any single stone mounted in a setting (whether of one or more stones).

Pearls

- Loose, with a minimum diameter of 3 millimeters per bead;
- Strung or mounted in a setting (whether of one or more beads), with a minimum diameter of 10millimeters per any single bead.

Other

The above definitions notwithstanding, for the purpose of applying AML/CFT measures in respect of covered transactions, the company will also consider PMs to include any object concerning which at least 50% of its monetary value is comprised of PMs.

Appendix 7 (a) See Federal Law No. (13) of 2004 on Controlling the Importation, Exportation and Transit of Raw Diamonds, as amended by Federal Law No. (4) of 2008.
Appendix 7 (b) See Decision of the Council of Ministers No. (45) of 2018 on the Executive Regulation of Federal Law No. (11) of 2015, on the Control and Stamping of the Trade in Precious Stones and Precious Metals, Annexes 1 and 2.

Furthermore, it should also be recognised that the company may engage in transactions involving other types of metals and gemstones (whether traded regularly or occasionally, and whether physically or through electronic or virtual exchanges) which, while technically not considered to be PMs (although they may be of high value in some cases), may nevertheless be subject to risks of ML/FT or other predicate offences (e.g. fraud) similar to PMs. Such materials may include:

- A variety of high-value industrial metals, including so-called conflict minerals (for example,wolframite, cassiterite, and coltan), cobalt, and other platinoid metals (e.g. rhodium, etc.);
- A variety of semi-precious gemstones (e.g. amethysts, opals, jade, and others);
- Synthetic, treated, or artificial gemstones (diamonds, emeralds, rubies, sapphires, pearls).

While this guidance focusses on the ML/FT risks associated specifically with PMs, the company will also takea similar risk-based approach to the application of AML/CFT measures in respect of covered transactionsinvolving these other types of metals and stones (since they can, in some situations, also be considered to pose ML/FT risks similar to those of PMs). In other words, the criterion for applying the required AML/CFT measures relates to the carrying out of monetary transactions which meet the threshold amount of AED 55,000.

APPENDIX 8: PURCHASE DECLARATION – CASH PURCHASE

On behalf of (Customer Name) declare that the source of cash for the purchase from AETERNO FZE on (Date of Purchase) is:

- ☐ Cash Retail Sales within UAE
- ☐ Cash Retail Sales Outside of UAE
- ☐ Cash Sales to Multiple Jewelry Wholesalers
- ☐ Cash Sales to Multiple Bullion Wholesalers
- ☐ Investor Capital
- ☐ Others (please specify)

In support of the above the following documents are being provided.

- ☐ For cash intensive business, company bank statements reflecting sizeable deposits as part of business as usual.
- ☐ Evidence of withdrawal from customer's own account (Company or Individual as the case may be). Bank Statement to be provided and reflecting withdrawal of amount for purchase.
- ☐ Money encashed at Exchange house, receipt & tourist visa.

Purpose of Purchase: (Customer Name) on (Date of Purchase)

- ☐ Retail Sales within UAE
- ☐ Export Retail Sales outside UAE
- ☐ Sales to Retailers within UAE
- ☐ Sales to Retailers outside UAE
- ☐ Sales to Jewelry Wholesalers in UAE
- ☐ Sales to Jewelry Retailers Outside UAE
- ☐ Sales to Bullion Dealers in UAE
- ☐ Sales to Bullion Dealers outside UAE
- ☐ Individual Consumption
- ☐ Others (please specify)

Yours Truly,

Authorized Signatory
Signature and Company Stamp

KEY DEFINITIONS:

Each firm Employee should know and understand the meaning of the terms in the below table from the Glossary module and the AML module.

FIU	FIU Means the Anti-Money Laundering Suspicious Cases Unit, the Financial Intelligence Unit of the U.A.E. Central Bank.
Beneficial Owner	A natural person or entity with sharehoding of a minimum of 10% or more.
Ultimate Beneficial Owner	UBOs are natural persons who ultimately own or control or have the right to vote with minimum 25% shareholding of the company, whether through direct or indirect ownership or who have the right to appoint or dismiss the majority of the Directors /Managers If no natural person satisfies the condition above, then any natural person who exercises control over the company through other means shall be deemed as the UBO If no natural person satisfies both conditions above, then a natural person who is responsible for the senior management of the company will be deemed as the UBO.
Supervisory Authority	Federal and local authorities which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and Non-Profit Organizations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations
Customer Due Diligence (CDD)	The process of identifying or verifying the information of a Customer or Beneficial Owner/Ultimate Beneficial Owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it.
Employee	Means an individual: 1. who is employed or appointed by a person in connection with that person'sbusiness, whether under a contract of service or for services or otherwise; or 2. whose services, under an arrangement between that person and a third party, areplaced at the disposal and under the control of that person.
Source of funds	Means the origin of customer's funds which relate to a transaction or service andincludes how such funds are connected to a customer's source of wealth

Suspicious Transactions	Transactions related to funds for which there are reasonable grounds to suspect thatthey are earned from any felony or misdemeanor, related to the financing of terrorismor of illegal organizations, whether committed or attempted.
Politically Exposed Person (PEP)	A natural person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, whether in the State or elsewhere, including but not limited to, a head of state or of government, senior politician, senior government, judicial or military official, ambassador, senior person in an International Organization, senior executive of a state owned corporation, an important political party official, or a member of senior management or an individual who has been entrusted with similar functions such as a director or a deputy director. This definition does not include middle ranking or more junior individuals in the above categories.
Source of Wealth	Source of wealth Means how the customer's global wealth or net worth is or was acquired or accumulated
Senior Management	Means, in relation to a Relevant Person every member of the Relevant Person's executive management.
FATF	Financial Action Task Force.
Designated Nonfinancial Businesses and Professions (DNFBP)	Anyone who conducts one or several of the commercial or professional activities i.e. • Auditors and accountants; • Lawyers, notaries and other legal professionals and practitioners; • Company and trust service providers; • Dealers in precious metals and stones; • Real estate agents and brokers; • Any other Designated Non-Financial Businesses and Professions (DNFBPs) notmentioned above.
OECD Due Diligence	OECD Due Diligence provides Guidance for Responsible Supply Chains of Mineralsfrom Conflict-Affected and High-Risk Areas
KYC Documentation - Individual	• Latest Emirates ID. • Passport. • Visa. • Proof of Residential Address in UAE (Utility bill or other bank statement fromlast 3 months)

KYC Documentation – Entity	• Emirates ID Card for all shareholders with > 5%. • Passport for all shareholders with > 5%. • Visa for all shareholders with > 5%. • Proof of Operating Address in UAE (Utility bill or other bank statement from last 3 months) • Trade License or Certificate of incorporation • Memorandum & Articles of Association (MOA/AOA) • Incumbency Certificate/Good Standing as applicable for the jurisdiction
SAR	• Report to be filled on the suspicion of an activity or an attempted transaction that was not executed
STR	• Report to be filled upon suspicion of a transaction