

ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM POLICY

This Manual is the sole property of ESTEEM BULLION - FZCO and is meant exclusively for its internal use. It is strictly forbidden to make or reproduce a copy of this Manual in any form, in part or in whole, without the prior written consent of the Owner/ Senior Management.



ESTEEM BULLION FZCO

VERSION : ESTEEM BULLION - FZCO/V2




Title	Anti-Money Laundering and Combating Financing of Terrorism Policy and Procedures
Information Classification	Internal
Policy Supported	ESTEEM BULLION FZCO
Current Version	v.2
Review Cycle	Annually
Due Date for Review	

Document Contact details

Role	Designation
Reviewed By	Senior Management
Approved	Owner

Policy Approval

The undersigned acknowledge that they have reviewed by Senior Management. Any further changes to this Policy in future can only be recommended by Senior Management and approved by Owner.

Document Title	ESTEEM BULLION FZCO	Signature
Prepared By	Compliance Deptment	
Reviewed By	HARSH VASANTHBHAI TANNA	
Approved By	HARSH VASANTHBHAI TANNA	







Abbreviations of Common Terms

Terms	Definitions
ML/TF	Money Laundering Means the process by which the financial proceeds of crime are disguised to conceal an illegal origin; Terrorist financing is the illegal smuggling of cash to terrorist organizations. Terrorist financing is often linked with money laundering, and it is not uncommon for it to be completed across international borders.
AML & CFT	Anti-Money Laundering. (As indicated earlier, all references in this document to AML will include obligations for Countering the Financing of Terrorism (CFT), Countering Proliferation Financing (CPF) and Other Identified Risks unless the context requires otherwise. The financing of terrorism involves the raising and processing of funds, from both legal and illegal sources, to supply terrorists with resources to carry out their attacks. While the phenomena differ in keyways, they often seek to exploit the same vulnerabilities that allow for an inappropriate level of anonymity and non-transparency in the execution of transactions.
AMLSCU	Anti-Money Laundering & Suspicious Cases Unit
FIU	Financial Intelligence Unit means the agency will collect raw transactional information and Suspicious activity reports (SAR) usually provided by banks and other entities as part of regulatory requirements.
DNFBPs	Designated Non-Financial Businesses and Professions (DNFBPs) Means Real estate agent & Dealers in precious metals. Dealers in precious stones. Lawyers, notaries, other independent legal professionals and accountants.
OECD Guidance	Organisation for Economic Co-operation and Development Means the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas;
Beneficial Owner	Beneficial Owner is defined in Article (5) of the Cabinet Decision No. (58) of 2020 Regulating the beneficial Owner Procedures: 1. “The Beneficial Owner of the Legal Person shall be whoever person that ultimately owns or controls, whether directly through a chain of ownership or control or by other means of control such as the right to appoint or dismiss the majority of its Directors, 25% or more of the shares or 25% or more of the voting rights in the Legal Person.” 2. The Beneficial Owner may be traced through any number of Legal Persons or arrangements of whatsoever kind. 3. If two or more natural persons jointly own or control a ratio of capital in the Legal Person, all of them shall be deemed as jointly owners or controllers of such ratio. 4. If, after all reasonable means have been taken, no natural person is identified as an ultimate Beneficial Owner in accordance with Clause (1) of this Article, or there is reasonable doubt that any natural person identified as an ultimate Beneficial Owner is the true Beneficial Owner in the Legal Person; then the natural person who controls the Legal Person by other means of control shall be deemed as the Beneficial Owner. 5. Where no natural person is identified in accordance with Clause (4) of this Article; then the natural person who holds the position of a higher management official shall be deemed as the Beneficial Owner
Client / Customer	A Client (identical meaning to Customer) should be understood as natural person or a legal person / entity with whom the reporting entity has a business relationship or for whom the reporting entity carried out an occasional transaction. In this context, customers refer to all existing customers with whom entity has had a business relationship within the reporting period including occasional (walk in) customers who have been serviced during the reporting period. Reference to customers is made in respect of those that were provided with a relevant activity or relevant service that falls under AML/CFT regulations by the reporting entity. For more information please see Cabinet Decision No. (10) Of 2019 concerning the implementing Regulation of Decree Law No. (20) Of 2018, Article 1 (definition of a "Customer), Article 2 and 3 (activities and transactions that fall under the scope of the AML/CFT regulations).



Governance	Governance related requirements are stipulated under AML/CFT Law No.20 of 2018, Article 16.1(d) and AML/CFT Cabinet Decision No. (10) of 2019, Article 4.2(a), 20, 21, 2 Term Definition 44.4 and AML/CFT guidance for Designated Nonfinancial Businesses and Professions (DNFBPs) issued by the Ministry of Economy (April 1, 2019), Article 8.
LLC.	LLC - Limited Liability Company; For definitions of different types of establishments please refer to Federal Law No 2 of 2015 on Commercial Companies
Resident	For the purpose of this questionnaire, a resident is a natural person who is a UAE national or who has a legal right to work and live in UAE, such as an appropriate visa holder.
Non Resident	For the purpose of this questionnaire, a non-resident is a natural person who is a non UAE national and who does not have a legal right to work and live in the UAE
“PEPs”	“Politically exposed persons” When individuals are elected to prominent political positions or assigned high-profile public roles, they should be categorized as politically exposed persons (PEPs) to reflect their increased risk of involvement in money laundering or terrorism financing.
DPEP	The FATF Guidance for PEPs also defines Domestic PEPs as high-risk individuals located in the same country as the financial institution of which it is a client and has a domestically located position. These domestic high-risk individuals are defined as officials of a local political party, senior politicians, heads of state companies, or senior military officials.
FPEP	“Foreign Politically exposed persons” Means persons holding an important public position on behalf of a government that differs from the government's public position in which the financial institution is located.
Proliferation Financing	Means providing funds or financial services for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.
TFS	Targeted Financial Sanctions are measures for asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of specified entities/ designated persons who are being sanctioned.
APG	The Asia/Pacific Group on Money Laundering is an inter-governmental organisation, consisting of 41 member jurisdictions. The objective of the APG is to ensure that individual members effectively implement the international standards against money laundering, terrorist financing and proliferation financing related to weapons of mass destruction.
FATF. “Financial Action Task Force”	The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard
EAG “Eurasian group on “	The Eurasian group on combating money laundering and financing of terrorism (EAG) is a FATF-style regional body which comprises 9 countries: Belarus, China, Kazakhstan, Kyrgyzstan, India, Russia, Tajikistan, Turkmenistan and Uzbekistan. EAG is an associate member of the FATF.
HSI	Homeland Security Investigations (United States) is the principal investigative arm of the U.S. Department of Homeland Security, responsible for investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel and finance move.
Jewellers	“Jewellers” means a person who is a bullion dealer or engaged in sale of jewelry, precious stones and metals including all articles made wholly or mainly of gold, platinum, diamonds of all kinds, precious or semi-precious stones, pearls whether or not mounted, set or strung and articles set or mounted with diamonds, precious or semiprecious stones or pearls.
Recycled Gold and/or Precious Metals	Means gold and/or precious metals that has been previously refined, such as end-user, post-consumer and investment gold and/or precious metals and gold and/or precious metals-bearing products, and scrap and waste metals and materials arising during refining and product manufacturing including recovered material from industrial recovery, which is returned to a refiner or another downstream intermediate processor to begin a new life cycle as ‘recycled gold’. The origin of Recycled Gold and/or Precious Metals is considered to be the point in the supply chain where the gold and/or precious metals is returned to the refiner or other



	downstream intermediate processor or recycler; assay samples are excluded from this category and falls out of scope of the review provided the member is able
Gold Bullion	Bullion means precious metal bars and coins (gold, silver, and platinum) that are designated for trading through their sale or purchase in units of ounces, kilograms and/or ten tolas and are considered high quality precious metals, unless stated otherwise by the company, and comply to the minimum purity requirements of the Dubai Good Delivery (DGD) and London Good Delivery (LGD) standards.
Gold Ingot	A gold bar, also called gold bullion or gold ingot, is a quantity of refined metallic gold of any shape that is made by a bar producer meeting standard conditions of manufacture, labeling, and record keeping. Larger gold bars that are produced by pouring the molten metal into molds are called ingots.
ASM	Artisanal and small-scale mining (ASM) is largely an informal sector with limited available information on production, revenues, operations and even location of activities. Regulation of the sector is often inadequate and its real contribution to a national economy is difficult to estimate.
LSM	Large-scale or medium-scale mining is governed by a framework of regulatory controls, permits and inspections and is subject to health, safety, social, environmental, closure and governance standards. Large-scale mining involves the payment of royalties and other taxes to governments in return for developing publicly-owned mineral resources.
CDD	"Customer due diligence" Means that part of the KYC process where information that comprises facts about a client is gathered by the dealer to assess the extent to which the client exposes the dealer to arrange of risks.
Transaction	Transaction is defined under Article 1 of the Cabinet Decision No. (10) Of 2019 "Transaction: All disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation." For the purpose of this questionnaire, transaction and payment should have an identical meaning.
Occasional Transaction	Any Transaction other than a Transaction carried out in the course of an established Business Relationship.
Suspicious transaction report	A suspicious transaction is a transaction that causes a reporting entity to have a feeling of apprehension or mistrust about the transaction considering its unusual nature or circumstances, or the person or group of persons involved in the transaction.
TBML Trade-based money laundering	Trade-Based Money Laundering takes advantage of the complexity of trade systems, most prominently in international contexts where the involvement of multiple parties and jurisdictions make AML checks and customer due diligence processes more difficult. TBML primarily involves the import and export of goods and the exploitation of a variety of cross-border trade finance instruments.
SAR:	Suspicious Activity Report



Table of Contents

1. Introduction	11
1.1 Basic Principles	11
1.2 Purpose & Scope	12
1.3 Definition	12
1.4 Covered Person of the Policy	12
1.5 Compliance and Enforcement of This Policy	13
1.6 Training and Awareness	13
2. AML/CFT LEGISLATIVE FRAMEWORK	14
2.1 The Financial Action Task Force (FATF)	14
2.2 The Middle East and North Africa Financial Action Task Force (MENAFATF)	14
2.3 Egmont Group of Financial Intelligence Units	14
2.4 Targeted Financial Sanctions	15
2.4.1 Types of financial sanctions	15
2.4.2 How to identify a match to apply TFS?	16
3. Definition of Key Terms	17
3.1 Money Laundering	17
3.2 The Three Stages of Money Laundering	17
3.3 Predicate Offenses	18
3.4 The Financing of Terrorism	19
3.5 Trade base Money Laundering	19
3.6 Attempted Transaction	21
3.7 Precious metals	21
3.8 Reporting Entity	21
4. Jewellers A Listed Business	21
5. As a Jeweler, your main obligations under the AML/CFT laws are summarized below:	22
6. Governance of Risk: Three Lines of Defense	25
7. Governance	25
7.1 Compliance Department	25
7.2 Compliance Programme	25
7.3 Independent Audit	26
7.4 Compliance Organization Chart	26
7.5 Role of Owner	26
7.6 Roles and Responsibilities of Compliance Officer	26
7.7 Money Laundering Reporting Officer – Responsibilities	27



7.8 Staff Screening and Training	28
7.8.1 Know Your Employees	28
7.8.2 Employee Screening	28
8. Training and Awareness	29
8.1 Objective	29
8.2 Training Material	29
8.3 Training Register	29
9. ML/FT Risk Assessment	30
9.1 Types of Risk	30
10. Mitigating Risk	34
10.1 Identification and Assessment of ML/FT Risks	34
10.2 Risk-Based Approach (RBA)	35
10.3 Overarching common requirements	35
10.4 Purpose and Objective:	35
10.5 Understanding of the RBA	36
10.6 Risk Factors	37
10.7 Risk Factors for the Precious Metals and Stones Sector	38
11. Risk Factors of Specific Concern to Dealers in Precious Metals/Stones	39
11.1 Stage of PMS Supply Chain & Role of DPMS	40
• Extraction/production	40
• Trading in raw minerals	40
• Beneficiation	41
• Wholesale trade	41
• Retail trade	42
12. Enterprise Risk Assessment	42
12.1 Conducting an enterprise risk assessment, as required by Article 4.1 of AML-CFT Decision	43
13. National Risk Assessment Summary	44
14. AML/CFT risk categories handling	45
15. Know-Your-Customer (KYC)	45
15.1 Updating Of KYC Information	46
15.2 Monitoring Of Clients' Activities	46
15.3 Customer Acceptance Policy	47
15.4 KYC Process has 3 stages:	47
16. Know Your Customer” Procedures and Control	48



16.1 Identification (ID), Verification (VR) and Know-Your-Customer (KYC)	49
16.2 Circumstances and Timing for Undertaking CDD Measures	50
16.3 Establishment of a Business Relationship	50
16.4 Occasional Transactions	51
16.5 Exceptional Circumstances	51
16.6 Customer Due Diligence (CDD) Measures	52
16.7 Customer and Beneficial Owner Identification/Verification	53
16.8 CDD Measures Concerning Legal Persons and Arrangements	54
16.9 Establishing a Customer Due Diligence Profile	55
16.10 Ongoing Monitoring of the Business Relationship	55
16.11 Reviewing and Updating the Customer Due Diligence Information	56
16.12 Enhanced Due Diligence (EDD) Measures	57
16.13 EDD Measures for High-Risk Customers or Transactions	58
16.14 Requirements for High-Risk Countries	59
16.15 Simplified Due Diligence (SDD) Measures	60
16.16 Reliance on a Third Party	61
17. Sanctions Screening	62
17.1 Data Management	63
17.2 The sanctions screening process	63
17.3 The importance of a data management cycle for effective sanctions screening	64
17.4 Sanctions screening data management	65
17.5 Sanction lists management	65
17.6 Challenges in managing data for sanctions screening	66
17.7 Potential solution and its benefits	67
17.8 Sanctions screening trends	69
A.1. Individual Customers	69
A.2. Corporate Customers	70
A.3 Know Your Customer (KYC) (Corporate Customer)	71
A.4 Attachment – To Be Filled In Only For Company Subject To AML - CFT Regulation	
74	
18. Suspicious Transactions/ Unusual Transactions	76
18.1 Obligation to Report Suspicious Transaction	77
18.2 Suspicious Transaction Reporting	77
18.3 Role of the Financial Intelligence Department	78
19. Politically Exposed Persons (PEPs)	79



20. Transaction Monitoring	81
20.1 Periodical Review	81
20.2 Trustee, Nominee Or Fiduciary Accounts	82
20.3 Transaction Undertaken On Behalf Of Account Holder or Non-Account Holders	82
21. Independent Review of Anti-Money Laundering Program	82
21.1 Introduction	82
21.2 Objectives	82
21.3 Guidelines	83
22. Red Flags	83
22.1 Red Flag Indicators for TF and PF	83
i. Red Flag Indicators for TF	83
A. Activity Inconsistent with the Customer’s Business:	83
B. Funds Transfers:	84
C. Other Transactions That Appear Unusual or Suspicious:	84
D. Terrorist Financing Indicators Published by FINTRAC (Canada’s Financial Intelligence Unit)	84
ii. Red Flag Indicators for PF	85
iii. Red Flag Indicators for Potential Sanctions Circumventions	86
23. Tipping off	88
24. Employee Behavior	88
25. Record Keeping	89
25.1 Required Record Types	90
26. Establishing an Effective Governance Framework	93
26.1 Adopt and Commit to a Policy for Managing Risks in Gold from CAHRAs	93
26.2 Establish Management Structures to Implement Supply Chain Due Diligence.	93
27. Identification and Assessment of the Supply Chain Risk	94
27.1 Conduct Supply Chain Due Diligence to identify potential risks	94
28. Management of the Supply Chain Risk	96
29. What are Targeted Financial Sanctions (TFS)?	96
29.1 What is United Nations Security Council Resolution (UNSCR)?	96
29.2 The FATF’s Commitment to TFS	97
29.3 What is Proliferation Financing of Weapons of Mass Destruction (PF-WMD)?	97
29.4 UN Security Council’s Approach to Counter TF and PF-WMD	97
29.5 UNSCRs which are Relevant to You as FIs	98
29.6 Legislation On Financial	98



29.7 The Obligation to Freeze ‘Without Delay’ defined	98
29.8 Protection against Liability for Reporting Persons	98
TFS are implemented in the UAE pursuant to UNSCRs in relation to:.....	99
29.9 Describe your jurisdiction’s sanctions regime.	100
29.10 There have been significant changes or developments impacting the UAE sanctions regime over the past 12 months.	100
A. Legal Basis/Sanctions Authorities	100
B. Jurisdiction implements United Nations sanctions.	101
C. Jurisdictions maintain any lists of sanctioned individuals and entities.	101
D. Can the public access those lists?	101
E. Comprehensive sanctions or embargoes against countries or regions	102
F. Jurisdiction maintains any other sanctions.	102
G. Implantation of Sanctions Laws and Regulations	102
H. Are parties required to block or freeze funds or other property that violate sanctions prohibitions?	102
I. Are there licenses available that would authorize activities otherwise prohibited by sanctions?	102
J. Are there any sanctions related reporting requirements? When must reports be filed and what information must be reported?	103
K. The government conveys its compliance expectations.	103
30 Money Laundering Penalties under UAE Federal Law no (20) of 2018	103



FOREWORD

It is the policy of ESTEEM BULLION FZCO to conduct its business in an honest and ethical manner. ESTEEM BULLION FZCO adheres to best practices with respect to Anti Money Laundering & Combating Financing of Terrorism Policy, and therefore it has a ZERO tolerance policy for Anti Money Laundering & Combating Financing of Terrorism done by employees, officers, directors, agents, consultants and contractors of ESTEEM BULLION FZCO

The purpose of this policy is to provide ESTEEM BULLION FZCO specific guidance for our organization on their legal obligations for measures to deter and detect money laundering and financing of terrorism activities. Because AML/CFT obligations are contained in several laws, amendments and regulations and as such laws, rules and regulations may have extra-territorial application, ESTEEM BULLION FZCO and its employees and associated persons will be bound by the most stringent of these requirements in respect of its and their conduct in all jurisdictions where they may operate, even if such conduct might otherwise be permitted by the local law of a particular jurisdiction.

ESTEEM BULLION FZCO will take all appropriate action under this Policy to ensure compliance with this Policy and applicable laws, rules and regulations, which may include disciplinary action, like reporting of violations of laws, rules and regulations to appropriate regulatory authorities. ESTEEM BULLION FZCO is committed to continual improvement and this document represents our first step towards establishing, implementing and maintaining a robust Anti Money Laundering & Combating Financing of Terrorism (“AML & CFT”) management system.



1. Introduction

Money laundering, terrorism and proliferation financing have far reached consequences for a country's financial system and economy. With these crimes becoming increasingly cross border in nature, jurisdictions must equip themselves to protect the integrity of our financial systems and must also be prepared to deal with any abuses which are encountered.

In order to achieve this, the first is a sound and robust legal framework, which empowers our company and lays down the obligations of all parties concerned.

The second is an open and collaborative approach between AML/CFT supervisors and the reporting persons that they regulate.

Additionally, we will be willingness from our company sectors which we will regulate to understand their obligations and to accept that they also have to contribute to the fight against ML and TF. Against this background, the FIU, as the AML/CFT regulator for the jewellery sector, firmly believes that one crucial way through which ML and TF can be curbed, is through the implementation of strong controls, policies and procedures by dealers.

The purpose of these guidelines is to assist our sector in establishing strong systems and in becoming partners in the fight against ML and TF. Its objective is also to help our company in understanding its AML/CFT obligations.

1.1 Basic Principles

The following principles should apply in the context of ESTEEM BULLION FZCO Anti Money Laundering & Combating Financing of Terrorism ("AML & CFT") Policy:

- a) It is ESTEEM BULLION FZCO policy to conduct all of its business in an honest and ethical manner. We take zero-tolerance approach to Money laundering and terrorism financing and we are very committed to acting professionally, fairly and with integrity in all our business dealings and relationships whenever we operate.
- b) It is our best practice objective that those we do business with take a similar zero-tolerance approach to Anti Money Laundering & Combating Financing of Terrorism ("AML & CFT").
- c) We are bound by the laws of the United Arab Emirates in respect of our conduct both at home and abroad and Businesses that deal with Gold, Silver and other precious metals are now required to meet the requirements set out in the UAE Law for Anti-Money Laundering and Combating Financing of Terrorism (AML-CFT).
- d) Since the risk factor is high, we will be performing regular client checks, monitor large transactions, and implement a robust AML compliance system within their organisation to ensure AML compliance. Since identifying the risks and adopting preventive measures are tough yet inevitable, the help of AML consultants in Dubai will come in handy for the gold dealers. Here is a detailed guide for the ESTEEM BULLION FZCO to ensure AML compliance and avoid AML penalties in the UAE.



1.2 Purpose & Scope

The purpose of this policy (the “Policy”) is to set out the responsibilities of ESTEEM BULLION FZCO and all employees in observing our commitment to the avoidance of Anti-Money Laundering and Combating Financing of Terrorism (AML-CFT). In developing the Policy, ESTEEM BULLION FZCO have made reference to the meet the AML / CFT obligations when they qualify as DNFBPs as defined in the Cabinet Decision No. (10) Of 2019, Concerning the Implementing Regulation of Decree-Law No. (20) Of 2018. As per the Cabinet Decision for Responsible Sourcing of Precious Metals and the LBMA (The London bullion market) Responsible Sourcing and Good Delivery Rules.

This Policy shall be complied with by all “Covered Persons”, namely (a) ESTEEM BULLION FZCO (b) all of its majority owned and controlled subsidiaries, associates, businesses or entities and (c) to all actions by their employees and shareholders. It covers dealings and transactions in all countries in which ESTEEM BULLION FZCO operates.

1.3 Definition

ESTEEM BULLION FZCO defines Anti-Money Laundering and Combating Financing of Terrorism (AML-CFT) as follows:

- a) the receiving or offering of an undue reward by or to any holder of public office, private employee, colleague, or representative of any other organization, designed to influence them in the exercise of their duty, and to incline them to act contrary to accepted standards of honesty and integrity; or
- b) the misuse of public office or public power for private gain or offering or promising anything of value, whether directly or indirectly, to a public official or a political candidate, party or party official, in order to obtain, retain or direct business, or to secure any improper business advantage. Also included is the demanding or accepting of anything of value by such a person as a condition to conferring an improper business advantage, whether directly or indirectly.

1.4 Covered Person of the Policy

ESTEEM BULLION FZCO Anti-Money Laundering and Combating Financing of Terrorism (AML-CFT) Policy requires Covered Person:

- a) Not to offer or make any bribe, unorthodox or unauthorized payment or inducement of any kind to anyone;
- b) Not to solicit business by offering any bribe, unorthodox or unofficial payment to customers or potential customers;
- c) Not to accept any kind of bribe, unorthodox or unusual payment or inducement that would not be authorized by ESTEEM BULLION FZCO in the ordinary course of its business activities;



- d) To refuse any bribe or unorthodox payment and to do so in a manner that is not open to misunderstanding or giving rise to false expectation; and to report any such offers to the Managing Director of ESTEEM BULLION FZCO

1.5 Compliance and Enforcement of This Policy

- This Policy was approved by the owner. The owner has overall responsibility for ensuring this Policy complies with our legal and ethical obligations, and that all those under our control comply with it.
- For the purposes of this Policy, the Compliance Manager is the Corporate Secretary. The Compliance Manager has primary and day-to-day responsibility for implementing this Policy, and for monitoring its use and effectiveness.
- Management and senior staff at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy.
- Employees are responsible to comply with ESTEEM BULLION FZCO policies and procedures and to be alert to any behavior or actions that are inconsistent with ESTEEM BULLION FZCO policies and procedures. Employees also are responsible to notify its superior or manager or the Compliance Manager of any suspected bribery and corruption.
- Top Management shall be the appointed custodian of this Policy and shall be ultimately responsible for the implementation and enforcement of this Policy.
- The ESTEEM BULLION FZCO shall appoint a compliance officer who will provide expertise and assistance regarding the implementation and enforcement of this Policy thus supporting the Top Management.

1.6 Training and Awareness

This Policy will be communicated to all employees during the initial staff induction process and as appropriate, thereafter in accordance with the commitment to ensure that all employees receive ongoing training. Our policy on Anti-Money Laundering and Combating Financing of Terrorism (AML-CFT) is supported by governance procedures covering monitoring of adherence and record keeping. Any breach of the Policy by any employee will be considered as grounds for disciplinary action, which may include dismissal.



2. AML/CFT LEGISLATIVE FRAMEWORK

2.1 The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) was established in 1989 by the G7 countries. It is an inter-governmental body whose purpose is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, financing of terrorism and other related threats to the integrity of the international financial system. The FATF standards are reflected in its 40 Recommendations issued in February 2012. These are universally recognized as international standards for anti-money laundering and countering financing of terrorism (AML/CFT).

The FATF issued a first report containing a set of Forty Recommendations, for the prevention of money laundering in April 1990. These 40 Recommendations were first revised in 1996. Subsequently, in October 2001 the FATF issued the Eight Special Recommendations to deal with the issue of financing of terrorism and added a ninth Recommendation in 2004.

The continued evolution of money laundering techniques led the FATF to revise the FATF standards comprehensively in June 2003. The revision brought a number of changes and one of the changes related to the classification of Dealers in Jewellery as Designated Non-Financial Businesses and Professions' (DNFBPs) by the FATF. This change means that Dealers in Jewellery are now subject to the same Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) requirements as casinos, real estate agents, lawyers. The most recent revision of the FATF recommendations was effected in 2012 and the 40+9 Recommendations were merged into 40 Recommendations.

2.2 The Middle East and North Africa Financial Action Task Force (MENAFATF)

The Middle East and North Africa Financial Action Task Force (MENAFATF) has been concerned also with this topic and decided to form an ad-hoc committee in April 2007 to study this topic and draft a guidelines to help member countries

For more information about the **MENAFATF**, please visit the website: www.menafatf.org.

2.3 Egmont Group of Financial Intelligence Units

The goal of the Egmont Group of Financial Intelligence Units (Egmont Group) is to provide a forum for financial intelligence units (FIUs) around the world to improve cooperation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field.

For more information about the **Egmont Group**, please visit the website: www.egmontgroup.org.



2.4 Targeted Financial Sanctions

The term targeted sanctions means that such sanctions are imposed against specific individuals or groups, or undertakings. The term targeted financial sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.

2.4.1 Types of financial sanctions

- **Asset freezing:** Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by listed individual, groups, or entities. It includes:
 - The Freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access.
 - The Freezing of economic resources also includes preventing their use to obtain funds, goods, or services in any way, including, but not limited to, by selling, hiring, or mortgaging them.
- **Prohibition to offer funds and services:** This means the prohibition to provide funds to, or render financial services or other services related to, any listed individual, group, or entity. This includes, for example, the opening of banking subsidiaries in the sanctioned jurisdictions, the provision of financial services or trading in natural resources (including oil) and providing internet and/or telecommunications services.
- **Asset freezing and prohibition** measures have no time limit: the funds must remain frozen, and the prohibition to offer funds and services stands until the individual, group, or entity is removed from the Local Terrorist List or the UN List or until there is a freezing cancellation decision made by a competent authority or the UNSC.

The target financial sanctions are implemented in the UAE following UNSCR with relation to:

- Terrorism and terrorist financing
- The proliferation of weapons of mass destruction (WMD)
- Other UN sanctions regimes with TFS



2.4.2 How to identify a match to apply TFS?

To identify must screen on an going basis, and at least daily, their customers, potential customers, beneficial owners, and transactions to identify possible matches to the Local Terrorist List or UN List. Sanctions Lists contain a range of information to aid the identification of listed individual or entity. The following are examples of the information contained in the Sanctions lists:

For Natural Person	For legal person
<ul style="list-style-type: none"> • Name • Aliases • Date of birth • Nationality • ID or Passport information • Last known address 	<ul style="list-style-type: none"> • Name (s) • Aliases • Address of registration • Address of branches • Other information

Because many are very common, you may find various potential matches. However, it does not necessarily mean that the individual or entity you are dealing with is subject to TFS.

When identifying the potential match, suspend any transaction until you can be satisfied it is not an individual or entity subject to TFS. (“False positive result”).

Note that: If the individual or entity you are dealing with matches all or most of the information on any of the Sanctions Lists, then this is likely to be a confirmed match. In this case, you must implement the freezing measures immediately, refrain from offering any funds or services, and notify the relevant Supervisory Authority and the Executive Office immediately.

- **Potential Match:** - A potential match is when there is any match between data in the Sanctions Lists with any information in your databases.
- **Confirmed Match:** - A confirmed match is when a potential match has been confirmed to be the individual, group or entity subject to TFS or when there is any doubt, indication, or suspicious that the potential match may correspond to individual, group or entity subject to TFS.
- **False Positive Result:** - False positive result is when a potential match was discharged.



3. Definition of Key Terms

3.1 Money Laundering

Money Laundering is the process by which funds derived from criminal activity (“dirty money”) are given the appearance of having been legitimately obtained, through a series of transactions in which the funds are ‘cleaned’. Its purpose is to allow criminals to maintain control over those proceeds and, ultimately, provide a legitimate cover for the source of their income.

For money laundering to take place, first, there must have been the commission of a serious crime which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies.

There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewellery) to passing money through legitimate businesses and “shell” companies or as in the case of drug trafficking or other serious crimes. The proceeds usually take the form of cash which needs to enter the financial system by some means.

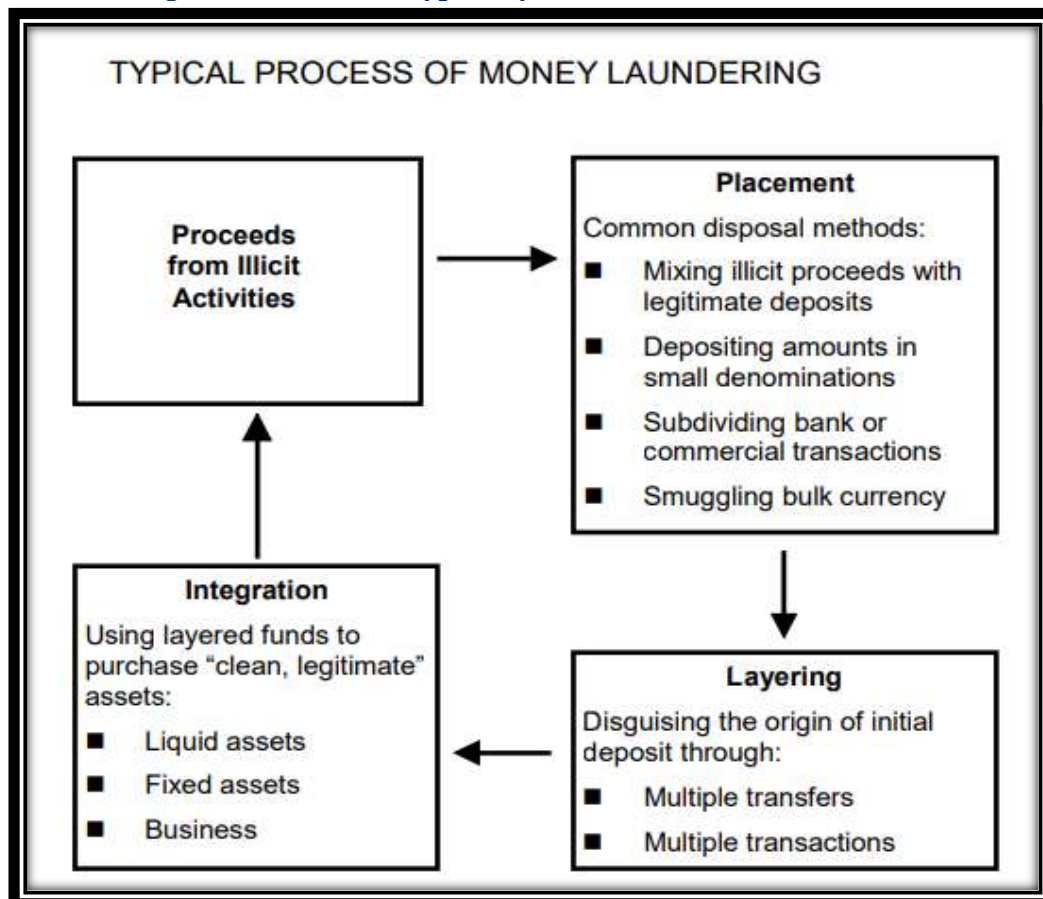
3.2 The Three Stages of Money Laundering

- I. Placement:** Criminally derived funds are brought into the financial system. In the case of drug trafficking, and some other serious crimes, such as robbery, the proceeds usually take the form of cash which needs to enter the financial system. Examples of Placement are depositing cash into bank accounts or using cash to purchase assets. Techniques used include Structuring - breaking up a large deposit transaction into smaller cash deposits and Smurfing – using other persons to deposit cash.
- II. Layering:** This takes place after the funds have entered into the financial system. It involves the movement of the money. Funds may be shuttled through a web of multiple accounts, companies and countries in order to disguise their origins. The intention is to conceal, hide, and obscure the money trail in order to deceive the law enforcement and to make the paper trail very difficult to follow. The more layers there are, the harder it is to detect the origin of the funds.



III. Integration: The money comes back to criminals as apparently legitimate funds. The laundered funds are used for activities such as investment into real estate, luxury assets, and business ventures, to fund further criminal activity or spent to enhance the criminal's lifestyle. At this stage, the illegal money has achieved the appearance of legitimacy. Successful money laundering allows criminals to use and enjoy the income from the criminal activity without suspicion.

IV. The following chart illustrates a typical cycle of ML



3.3 Predicate Offenses

The AML-CFT Law defines a predicate offence as "any act constituting an offence or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries." A predicate offence is therefore any crime, whether felony or misdemeanor, which is punishable in the UAE, regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

FATF has designated 21 (twenty-one) major categories comprising many individual predicate offences. Each of these categories of predicate offences has been criminalised in the legislative framework of the State. Supervised institutions are reminded that this is not an exhaustive list of predicate offences, but simply a convenient categorization, since in the UAE according to the



AML-CFT Law, even crimes that do not appear on this list, whether felonies or misdemeanors, can be predicate offences to money laundering.

Based on expert analysis of these categories conducted on behalf of the UAE's Competent Authorities for the 2018 National Risk Assessment, the top (highest) threats to the State in relation to money laundering have been identified as: fraud, counterfeiting and piracy of products, illicit trafficking in narcotic drugs and psychotropic substances, and professional third-party money laundering

3.4 The Financing of Terrorism

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity. Funds may involve low dollar value transactions and give the appearance of innocence and a variety of sources. Funds may come from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organize fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, all the funds are actually transferred to a terrorist group. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism you may have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place are Supervised.

However, like money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. The reason is to prevent leaving a trail of incriminating evidence - to distance the funds from the crime or the source, and to obscure the intended destination and purpose.

Offering, collecting, ensuring access to, or transporting funds by any direct or indirect means to any society, organization, establishment, center, group, gang or any other persons to whom the provisions of Federal Law No. (7) Of 2014 regarding terrorist acts, apply. The UAE, cognizant of the need for regulatory legislation, has enacted numerous laws at federal level to prevent and criminalize money laundering and the financing of terrorism.

3.5 Trade base Money Laundering

The value of precious metals and stones varies highly based on their quality and purity, features which may not be apparent to the naked eye. In addition, the value of certain precious stones, particularly diamonds, can differ for different non-industry customers based on their personal preferences. This makes precious metals and stones particularly vulnerable to TBML, in which illicit actors use supposedly or actually licit trade to hide illicit finance.



- Trading the same goods—often precious stones—repeatedly between co-conspirators to justify funds transfers between members of a criminal network, or between companies owned by the same individual(s). In these schemes, a single precious stone may be repeatedly sold between members of the network, or a single stone may be sold to multiple “purchasers” at the same time, each time with a different description.
- Inflation or deflation of the value of traded stones to provide justification for cross-border transfers. A merchant may sell low-value precious metals or stones to a purchaser, but invoice for higher-quality goods and thus a higher sum. The purchaser pays the full invoice price, justifying the transaction to financial institutions, and also receives illicit goods such as drugs or smuggled items.
- Use of precious metals and stones as security for fraudulent loans. In a typology that is often related to TBML, precious metals or stones may be repeatedly sold or falsely valued between members of a network in order to justify loans and other forms of financing.



- Trading gold to legitimize the proceeds of drugs trafficking.
- Large –Scale sanctions evasion using precious metals.
- Over valuation



3.6 Attempted Transaction

Is one where a customer intended to conduct a transaction and took some form of action to do so it is different from a simple request for information, such as an enquiry as to the price of a certain item? An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.

3.7 Precious metals

Include, but are not limited to bullion, platinum, gold and silver coins, and jewellery made from same.

Precious stones include but are not limited to diamonds, rubies, precious and semiprecious stones and man-made gemstones.

3.8 Reporting Entity

If a DNFBP suspects, or has reasonable grounds to suspect, that any transaction, proposed transaction or attempted transaction is related to ML/TF or other serious crime, our company required to immediately file a Suspicious Transaction Report (STR) to the FIU.

4. Jewellers A Listed Business

The FATF, the body which sets standards internationally for money laundering and financing of terrorism, in evaluating risks and vulnerable activities has found that money laundering and financing of terrorism activities have involved precious metals and precious stones. A dealer in precious metals and precious stones has been identified as a business which is vulnerable.

Precious metals and stones, particularly gold and diamond, offer a high intrinsic value in a compact form. They can be “cashed” easily in most areas of the world. Hence, they are vulnerable to be used in money laundering for the ease in which they can be hidden and transported.

Terrorist groups have engaged in the gemstone trade for a long time. Historically, they engaged extensively in the profitmaking trade in diamond, tanzanite, amethyst, ruby and sapphire. However, according to recent intelligence, gemstones, diamonds in particular, are being used as a way of storing terrorist assets outside the formal financial sector. The aim is no longer only in turning a profit but also acquiring as many stones as possible with crime proceeds that are being kept out of banks and businesses.

FATF has acknowledged the vulnerability of dealers in precious metals and precious stones by recommending that such business activity should be subject to AML/CFT requirements. All countries in the world have to have laws which put these requirements on Jewelers.



5. As a Jeweler, your main obligations under the AML/CFT laws are summarized below:

- **Register with the FIU:** ESTEEM BULLION FZCO must register with the FIU for the purpose of identifying yourself as an entity which is supervised by the FIU if you perform any of the specified activities. You must also notify the FIU of a change of address of your registered office or principal place of business.
- **Submit Reports to the FIU:** There are two (2) types of FIU reports
 - I. Reports of Suspicious Transactions or Activities; and
 - II. Reports of Terrorist Funds in your possession.
- **No “Tipping-off”:** When company have made a suspicious transaction report to the FIU, you or any member of your staff must not disclose that you have made such a report or the content of such report to any person including the Customer. It is an offence to deliberately tell any person, including the Customer, that you have or your business has filed a suspicious transaction report about the Customer’s activities/transactions. Company will not disclose to anyone any matter which may prejudice money laundering or financing of terrorism investigation or proposed investigation.
- **Keep Records:** Company are required to keep a record of each and every transaction for a specified period. Record keeping is important to anti-money laundering investigation which allows for swift reconstruction of individual transactions and provides evidence for prosecution of money laundering and other criminal activities.

As per Article 24 of Cabinet Decision No. 10 of 2019: records in electronic or written form for a period of five (5) years or such longer period as the FIU directs. The records must be kept for five (5) years after the end of the business relationship or completion of a one-off transaction.

- All domestic and international transaction records;
- Source of funds declarations;
- Customer’s identification records;
- Customer’s information records;
- Copies of official corporate records;
- Copies of Suspicious Transaction Reports submitted by your staff to your Compliance Officer (STRs/SARs);
- A register of copies of suspicious transaction reports submitted to the FIU (STRs/SARs);
- A register of all enquiries made by LEAs (date, nature of enquiry, name of officer, agency and powers being exercised) or other competent authority;
- The names, addresses, position titles and other official information pertaining to your staff;)
- All Wire transfers records; (originator and recipient identification data) and
- Other relevant records.



- **Ascertain customer identity: Know Your Customer:** If you cannot satisfactorily apply your due diligence measures in relation to a Customer, e.g., you are unable to identify and verify a Customer's identity or obtain sufficient information about the nature and purpose of a transaction, you must NOT carry out a transaction for that Customer or enter into a business relationship with the Customer and you must terminate any business relationship already established. You should also consider submitting a STR/SAR to the FIU.
- a) **All Customers:** - Identify who is the prospective customer and verify the person's identity by reference to independent and reliable source materials. Such material should include documentary identification issued by the Government departments or agencies. Company must also ask the source of funds for the transaction. Customer's identification, also called CDD or Know Your Customer-KYC, must be obtained for customers who are individuals as well as companies. You must obtain satisfactory evidence of the Customer's identity before establishing a business relationship or completing a transaction for occasional customers.
- b) **High Risk Customers/Transactions:** - There are customers and types of transactions and products which may pose higher risk to your business and Company will take additional measures in those cases. The AML/CFT laws have identified certain high risks customers and require you to conduct Enhanced Due Diligence ("EDD") on these customers. You may also determine that certain customers, transactions and products pose a higher risk to your business and apply EDD. Company will take specific measures to identify and verify the identity of the following individuals or entities.
- c) **Transaction with resident individual customer:** - Obtain identification documents (Emirates ID or Passport) for cash transaction or wire transfer equal or exceeding AED 55,000 and register the information in the Financial intelligence Units (FIU) GoAML platform using the recently DPMSR within 15 days
- d) **Transaction with nonresident individual:** - Obtain identification documents (Emirates ID or Passport) for cash transaction or wire transfer equal or exceeding AED 55,000 and register the information in the Financial intelligence Units (FIU) GoAML platform using the recently DPMSR within 15 days
- e) **Transaction with entities /Companies:** - Obtain a copy of the trade license, identification documents (Emirates ID or Passport)of the person representing the company, for cash transaction or wire transfer equal or exceeding AED 55000 and register the information in the Financial intelligence Units (FIU) GoAML platform using the recently DPMSR within 15 days.
- f) Keep records of all the documents and information in the FIU GOAML using the newly created account



EDD measures to apply to high risk customers include but is not limited to:

- ❖ Verification of identity using independent sources e.g., additional form of Government issued identification;
- ❖ Obtaining details of the source of the customer's funds and the purpose of the transaction;
- ❖ Obtaining approval from the senior officer to conduct the transaction;
- ❖ Applying supplementary measures to verify or certify the documents supplied or requiring certification by a financial institution;
- ❖ Imposing a cash threshold limit for transactions after which a senior officer's approval is needed to conduct the transaction;
- ❖ Verifying the source of funds for the transaction e.g., if Customer states the money is from his bank account, ask for proof.
- ❖ Ongoing monitoring (e.g., monthly, quarterly or on a transaction basis) of the Customer's account through the relationship; or
- ❖ Obtaining details about the source of items in pawn-broking transactions

➤ **Ascertain whether the customer is acting for a Third Party:**

Company must take reasonable measures to determine whether the Customer is acting on behalf of a third party especially where company have to conduct EDD.

Such cases will include where the Customer is an agent of the third party who is the beneficiary and who is providing the funds for the transaction. In cases where a third party is involved, you must obtain information on the identity of the third party and their relationship with the Customer.

In deciding who the beneficial owner is in relation to a Customer who is not a private individual, (e.g., a company) you should identify those who has ultimate control over the business and the company's assets such as the shareholders.

- **Appoint a Compliance Officer;**
- **Develop an effective Compliance Programme and submit to the FIU; and**
- **Implement your Compliance Programme and conduct periodic reviews.**



6. Governance of Risk: Three Lines of Defense

ESTEEM BULLION FZCO has three line of defense which is appropriate for an organization irrespective of size and complexity.

In ESTEEM BULLION FZCO we organize the governance and management framework according with the regulatory guidelines.

- Operations - The first line of defense- functions that owns and manage risk
- Compliance – Is the second line of defense functions that oversee or specialize in risk Management and compliance
- Internal Audit - The third line of defense functions that provide independent assurance above all internal audits.

7. Governance

7.1 Compliance Department

ESTEEM BULLION FZCO the Owner sets the tone at the top, for compliance environment and culture. Following are the roles and responsibilities of the Key members, committee and employees of the organization:

7.2 Compliance Programme

The following seven (7) elements must be included in your compliance regime

- The appointment of a staff member as CO;
- Internal compliance policies and procedures;
- Your assessment of your risks to money laundering and terrorism financing, and measures to mitigate high risks;
- Ongoing compliance training for staff; and
- Periodic documented review of the effectiveness of implementation of policies and procedures, training and risk assessment.
- Ensuring independent audit of the compliance programme and the activities of the compliance officer.
- Such reviews (both internal and external) must be documented and made available.



7.3 Independent Audit

Putting your AML/CFT Compliance programme in place is not enough. The programme must be monitored and evaluated.

Therefore, our company will have an independent audit performed by people not involved with the entity's AML/CFT Compliance staff to test compliance with the procedures, policies and controls. The individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors.

7.4 Compliance Organization Chart



7.5 Role of Owner

- The Owner is overall responsible for implementing the robust compliance program across each business product, counterparty, country in which it deals, delivery channel of its services, customers etc.
- The Owner ensures that the company has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- The Owner approves the overall business risk assessment for ESTEEM BULLION FZCO
- The Owner reviews the compliance report along with high-risk areas.
- The Owner ensures that all employees of the organization are being trained on the AML/CFT.
- The Owner approves the AML/CFT policy.
- The Owner reviews the Compliance issues raised by the Compliance Officer.

7.6 Roles and Responsibilities of Compliance Officer

- Solely responsible for creating and implementing the AML/CFT Sanction compliance program for ESTEEM BULLION FZCO and ensuring compliance with AML/CFT Sanction Laws, Regulations, Notices, the Standards, and International laws
- Making sure ESTEEM BULLION FZCO is prepared with appropriate AML/CFT Sanction policies, procedures, processes, and controls.
- Compliance of the business against internal AML/CFT Sanction policies and procedures in day-to-day activities is implemented
- Assess all suspicious transaction alerts from employees and take appropriate decisions to report all suspicious cases to the FIU.
- Transaction Monitoring to identify high-risk, unusual, and suspicious customers/transactions
- Submission of Suspicious Transaction Reports to the FIU in a timely.



- Provide support and assistance to FIU with all information it requires for fulfilling their obligations.
- Ensure submission of Suspicious Transaction Reports to the FIU in a timely manner. Anti-Money Laundering & Combating Financing of Terrorism Policy
- Ensure the Cooperation with and provide the FIU with all information it requires for fulfilling their obligations.
- Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters (whether internal or external) and developing AML Training calendar for ensuring all staffs are adequately trained.
- Reviewing and sharing input with compliance reports on the effectiveness of the AML / CFT controls.
- On-going monitoring of what may, in his opinion, constitute high-risk customer accounts, suspicious customers/transactions.
- Ensure that CO is maintaining all necessary CDD, transactions, STR and staff training records for the required periods.
- Ensure all key documents pertaining to KYC of customers, customer transactions and STR are retained for the minimum period of 5 years.

7.7 Money Laundering Reporting Officer – Responsibilities

- Customer onboarding and KYC documentation
- Conducting Customer Due Diligence and Enhanced Due Diligence
- Transaction Monitoring and escalations
- Investigate Internal Suspicious Transaction Reports (ISTR)
- Assist in filing periodic reports with the FIU
- Monitoring trade-based money laundering and tracing structured transactions.
- Investigate, research, and act for the exceptions for name clearance & monitoring of payment transactions.
- Maintain appropriate records and arrange monitoring of suspicious accounts periodically.
- Assist in training to the entire staff of the organization
- Provide support and advice to other departments in relation to the application of ML rules and regulations to their function.
- Should be familiar with branch operations.
- Review and address Watch list and alerts. Update the blacklists on a regular basis.
- Liaison with the compliance department of the correspondent bankers and satisfactorily answer any queries posed.
- Create sound internal controls and monitor adherence to them Collaborate with HR when needed.
- Execution of the regulations issued by MOE and the organization's AML/CFT policies & procedures
- Performing more extensive, due diligence for high-risk amounts/ countries/ customers and include proactive monitoring for suspicious types of activities.
- Educating the staff in the branches regarding AML/CFT 'know your customer's procedures
- Maintaining records as required by ESTEEM BULLION FZCO AML/CFT policy & procedures.



7.8 Staff Screening and Training

7.8.1 Know Your Employees

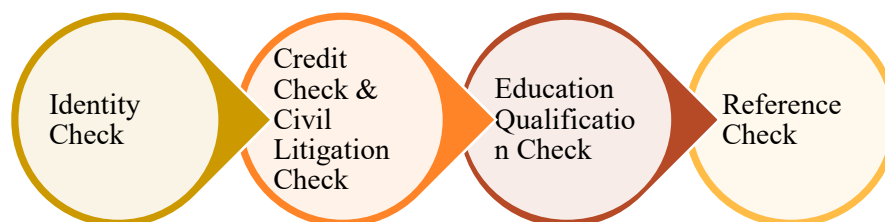
To ensure a high level of competence and AML/CFT programme effectiveness, ESTEEM BULLION FZCO should formulate and implement appropriate policies, procedures and controls with regard to staff screening and training.

These measures should be applied across organisation's and financial groups, including their foreign branches and majority-owned subsidiaries. Examples of some of the factors that should be considered when determining appropriate staff screening and training measures include, but are not limited to:

- ❖ The results of the NRA;
- ❖ The nature, size, complexity, and risk profile of ESTEEM BULLION FZCO industries and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;
- ❖ Effective screening and selection methods in relation the AML/CFT cultural compatibility of their employment candidates;
- ❖ Assessment of staff AML/CFT competency in relation to training and development needs;
- ❖ The type, frequency, structure, content, and delivery channels of AML/CFT training programmes and development opportunities;
- ❖ The effective identification, deployment and management of both internal and external training resources;
- ❖ Appropriate methods and tools for assessing the effectiveness of staff hiring, training, and development programmes.

7.8.2 Employee Screening

Before the final offer is issued, the ESTEEM BULLION FZCO may perform the following checks on the shortlisted candidate, after taking their consent:



- ❖ **Identity Check/Passport Check:** - Criminal Check (Good Conduct Certificate from Police of UAE/countries where the employee will be joining, for the last 5 years).
- ❖ **Credit Check & Civil Litigation Check:** - Al Etihad Credit Bureau in UAE and other similar agencies in countries, where the candidate is joining from.



- ❖ **Education Qualification Check:** - We only take the attested document of their educational qualification. In case the job does not require educational qualification, we waive this clause off.
- ❖ **Reference Check:** - We perform a reference check on the employee's previous employers

8. Training and Awareness

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

A comprehensive AML/CFT training is also provided to owners. The regular training received by our employees covers this policy the KYC procedures, the UAE and international regulations, the identification and reporting of suspicious transactions. Our policy is to provide all relevant employees with AML training within Thirty (30) days of joining the company.

8.1 Objective

Employees include customer contact employees, operational staff and senior management. The objective and content of the AML Training program as well as the development of training program and calendar are the responsibility of the Compliance Officer.

In ESTEEM BULLION FZCO, we ensure that the Compliance Officer must undergo AML/CFT training as stipulated by the Regulations.

- ❖ Mandatory induction training on AML/CFT sanctions and fraud for all new hires.
- ❖ To upgrade the Product Knowledge of Front line / Operations & Support Services.
- ❖ For all other employees, refresher training at regular intervals.
- ❖ As and when there are changes in the AML/CFT Sanction laws or regulations.

8.2 Training Material

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

8.3 Training Register

The Compliance Officer will maintain the record of attendance of all conducted training sessions.



9. ML/FT Risk Assessment

This Policy contains, as an integral part to it, certain procedural checks and balances (collectively, “Procedures and Controls”) to ensure the vigilant and effective operation of the Policy.

At ESTEEM BULLION FZCO, we understand, assess and identify the money laundering and terrorism financing associated with our everyday business on a day-to-day basis. We implement a sound ML/FT risk assessment methodology as to suit the size, nature and complexity of the daily business. We employ additional parameters which are relevant to nature, size, and complexity of our business before we enter into a new business relationship and in order to identify and assess ML/FT Risks.

Our company forms time to time undertake on and off-site inspections to reporting entities to monitor how the AML/CFT Compliance programmes are being implemented.

9.1 Types of Risk

Dealers may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling dealers, where required, to subject each client to reasonable and proportionate risk assessment. During the course of a client relationship, procedures for ongoing monitoring and review of the client/transactional risk profile are also important.

There are certain types of risk that are of particular importance to dealers since there are peculiar to this line of business:

- **Regulatory Environments:** Environmental risk considers the external and internal environments that an organisation operates in UAE

The methodology facilitates an assessment of the predicate crimes that can give rise to ML/TF, identified by international guidance, which an organisation can be vulnerable. This vulnerability may be because a customer is involved in the commission of one or more predicate crimes and/or is seeking to use products and services to launder the proceeds of a predicate crime.

The methodology has grouped predicate crimes into several categories to assist the assessment. The grouping includes deceptive crimes, illicit trafficking, property crimes, and crimes against the person (personal crimes).

The ML/TF environmental risk methodology also includes the internal vulnerability of the organisation to being used to launder money, finance terrorism, or breach targeted financial sanctions.

In addition, the ML/TF environmental risk methodology considers the organisation’s vulnerability to non-compliance with relevant AML/CFT law and regulation, if it does not put in place appropriate controls or implement adequate responses to AML/CFT obligations. Environmental ML/TF risk is assessed at the inherent risk and residual risk level.



Inherent environmental risk

Inherent environmental ML/TF risks are assessed and rated through the AML Accelerate platform by applying a combination of risk likelihood and risk impact, using the following matrix:

Environmental Inherent Risk Rating (IRR)		Impact			
		Minor	Moderate	Major	Unknown
Likelihood	Very likely	Medium	High	Significant	High
	Likely	Low	Medium	High	High
	Unlikely	Low	Low	Medium	High
	Unknown	High	High	High	High

The methodology defines and applies consistent criteria for both the likelihood and impact when assessing inherent environmental ML/TF risk:

Likelihood		
Very likely	Almost certain that the risk will occur several times a year.	A risk is very likely if it has occurred previously and may also occur in the near future.
Likely	High probability the risk will occur at least once.	A risk is likely if it has occurred previously and is likely to occur again
Unlikely	Unlikely if not impossible the risk will occur.	A risk is unlikely if it has not occurred previously and is not expected to occur.
Unknown	Do not know the likelihood of the risk occurring.	If you do not know or are unsure whether a risk will occur the likelihood is unknown.
Impact		
Major	Major damage or effect should it occur. Serious consequences for the business or compliance with AML/CFT obligations or vulnerable to serious terrorist act or large-scale money laundering risk	A major impact means the risk could result in significant financial penalties (with reference to the size and profitability of the business) or limitations or restrictions on business activities that could affect the businesses ability to continue as a going concern.
Moderate	Moderate damage or effect should it occur. Moderate consequences for the business or compliance with AML/CFT obligations or some level of money laundering or terrorism financing risk.	A moderate impact means that whilst the risk could result in financial penalties or limitations or restrictions on business activities These would not affect the businesses ability to continue as a going concern
Minor	Minor or negligible consequences or effects should it occur. Low level of money laundering or terrorism financing risk	A minor impact means that any financial penalties or limitations or restrictions on business activities are not material
Unknown	Do not know the impact, or have not assessed the impact of it occurring.	If you do not know or are unsure what the impact will be the impact is unknown.



The methodology defines and applies consistent criteria when assessing inherent environmental ML/TF risk:

Rating	Inherent Risk Rating
Significant	Major ML/TF risk.
High	Serious ML/TF risk
Medium	Moderate ML/TF risk.
Low	Minor or negligible ML/TF risk.

Residual environmental risk

Residual environmental ML/TF risks are assessed and rated through the AML Accelerate platform by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate that risk, using the following matrix:

Environmental Residual Risk Rating (RRR)		Control Assessment			
		Excellent	Adequate	Poor	No Control/Not Tested
Environmental Inherent Risk Rating (IRR)	Significant	Medium	High	Significant	Significant
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

The methodology defines and applies consistent criteria when assessing the effectiveness of controls as part of a residual environmental ML/TF risk:

Control Assessment	
Excellent	Highly effective controls. Controls in place are state of the art controls necessary to mitigate the risks and the controls appear to be working highly effectively at mitigating the risk.
Adequate	Effective controls. Controls in place are the right controls necessary to mitigate the risk and the controls appear to be working sufficiently.
Poor	Ineffective controls. Controls in place but not the right controls necessary to mitigate the risk or the controls appear not to be fit for purpose.
No Control/Not Tested	No controls in place or the effectiveness of the controls in place has not been tested.



The methodology defines and applies consistent criteria when assessing residual environmental ML/TF risk:

Rating	Residual Risk Rating (RRR)
Significant	Risk almost sure to occur and/or to have major consequences, and inadequate controls in place to mitigate the risk.
High	Risk likely to occur and/or to have serious consequences, and adequate controls in place.
Medium	Possible this could occur and/or have moderate consequences, and adequate or excellent controls in place.
Low	Unlikely to occur and/or have minor or negligible consequences, and adequate or excellent controls in place.

- **Country or geographic risk**: The risks associated with the jurisdictions in which the customer lives (for individuals) or is registered/headquartered (for legal persons) and where it operates, including the jurisdictions where it has subsidiaries, where it sources its products (where relevant), and where its main counterparties are based. These may include the overall risk of money laundering, terrorist financing, and financing of proliferation, as well as what is known regarding the prevalence of abuse of entities in these sectors.
- **Customer and counterparty risk**: For our company customer risk can be assessed as the proportion of higher-risk customer types (e.g. PEPs, legal persons, and customers from high-risk jurisdictions) within a customer's customer base.
- **Product, Service, and Delivery Channel Risk**: Company have assess risk in this category on two dimensions:
 - a) The products and services that the customer offers to its customers, and the delivery channels through which it offers these products and services. Products, services, and delivery channels that promote the rapid, anonymous transfer of high values are particularly attractive to illicit actors.

These may include, but are not limited to:

- i. Online/non-contact sales: Non-face to face transactions make it easier for criminals to hide their identities.
- ii. Accepting cash for high-value purchases. Cash is very difficult to trace and can be exchanged without involving the formal banking system, and thus is particularly attractive to criminals.
- iii. Accepting virtual assets: Virtual assets, like cash, are anonymous and difficult to trace to their users. Unlike cash, virtual assets allow parties to carry out transactions even when they are at a distance from one another. These qualities, combined with the lack of consistent regulation of entities that deal in virtual assets, make virtual assets high risk for abuse by illicit actors.



- b) The ESTEEM BULLION FZCO products and services that the customer intends to use, and the delivery channels through which the company will provide these services. Company have drawn on their entity risk assessment to assess the risk of the products and services each customer uses or intends to use.

- **Controls Risk:** ESTEEM BULLION FZCO understand the regulatory requirements in place for the customer, as well as how well they are enforced. In addition, participants in the precious metals and stones sector may also be required to comply with UAE requirements or global standards related to sourcing precious metals and stones and transparency of supply chains.

Where relevant to a customer's business, our company consider whether our customer conducts appropriate supply chain due diligence

In addition to risk rating customers, company also consider the risks of specific transactions, especially high-value transactions, those involving high-risk jurisdictions, and those that represent departures from a customer's standard or expected behavior. The company is aware of sectoral risks when reviewing large transactions associated with the DPMS or transactions of any size that do not have a clear licit economic purpose.

10. Mitigating Risk

ESTEEM BULLION FZCO have implemented appropriate measures and controls to mitigate the potential money laundering and terrorist and proliferation financing risk of those customers that are determined to be a higher risk as a result of the dealers' risks assessment. The same measures and controls may often address more than one of the risk criteria identified and it is not necessarily expected that dealers establish specific controls that target each criterion. Appropriate measures and controls may include:

- ❖ General training for appropriate personnel on money laundering and terrorist and proliferation financing methods and risks relevant to dealers.
- ❖ Targeted training for appropriate personnel to increase awareness of higher risk customers or transactions.
- ❖ Increased levels of know your customer/counterparty (KYC) or enhanced due diligence.
- ❖ Escalation within dealer management required for approval.
- ❖ Increased monitoring of transactions.
- ❖ Increased controls and frequency of review of relationships.

10.1 Identification and Assessment of ML/FT Risks

ESTEEM BULLION FZCO are obliged to identify, assess, and understand the ML/FT risks to which they are exposed. Both the AML-CFT Law and the AML-CFT Decision provide that supervised institutions may utilize a risk-based approach with respect to the identification and assessment of ML/FT risks. Guidance on these subjects is provided in the following sections.

Identifying ML/TF risks facing a firm, given its customers, services, countries of operation, also having regard to publicly available information regarding ML/TF risks and typologies.



10.2 Risk-Based Approach (RBA)

Risk Based Approach (RBA) “Risk Based Approach in AML/CFT means the identification, Understanding and Assessment of ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and combating the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations.

10.3 Overarching common requirements

Company have taken a risk-based approach to the preventive measures they put in place for all customers, including customers in the precious metals and stones sectors. A risk-based approach means that our company have dedicate compliance resources and effort to customers, business lines, branches, and products and services in keeping with the risk presented by those customers, business lines, branches, and products and services, as assessed in accordance with Article 4 of AML-CFT Decision.

10.4 Purpose and Objective:

- ❖ Inculcate awareness and understanding of what the risk-based approach involves.
- ❖ Outline the high-level principles involved in applying the risk-based approach.
- ❖ Indicate good practice in the design and implementation of an effective risk-based approach.

➤ Target audience

- ❖ Dealers in precious metals and stones which include persons
- ❖ Who produce precious metals or precious stones at mining operations,
- ❖ Intermediate buyers and brokers
- ❖ Precious stone cutters and polishers and precious metal refiners, To Jewellery manufacturers who use precious metals and precious stones,
- ❖ Retail sellers and to the public,
- ❖ Buyers and sellers in the secondary and scrap markets.
- ❖ SRO/Association of dealers



10.5 Understanding of the RBA

Risk is defined as the possibility of some adverse event occurring and the likely consequences of this event. Risk is expressed as;

- ❖ Combination of threat and vulnerabilities



- ❖ Risk is also defined as Risk = Likelihood x Consequence
- ❖ **ML threat refers to:** The proceeds of crimes in a country which includes

The proceeds generated in the country (internal threat)

The proceeds that come from other countries (external threat)

- ❖ **ML Threat Assessment should analyze:**

The frequency of predicate crimes that generate illicit proceeds.

The scale of illicit proceeds in the country

The scale of ML in the country

ML methods and trends in the country

- ❖ **TF threat:**

Refers to the scale of funds raised/ moved/used or utilized/transiting to support TF activities and groups

- ❖ **Vulnerability:** Is the state of being exposed to weaknesses and gaps in defense mechanisms against ML/TF, which can be at the national and/or sector level.

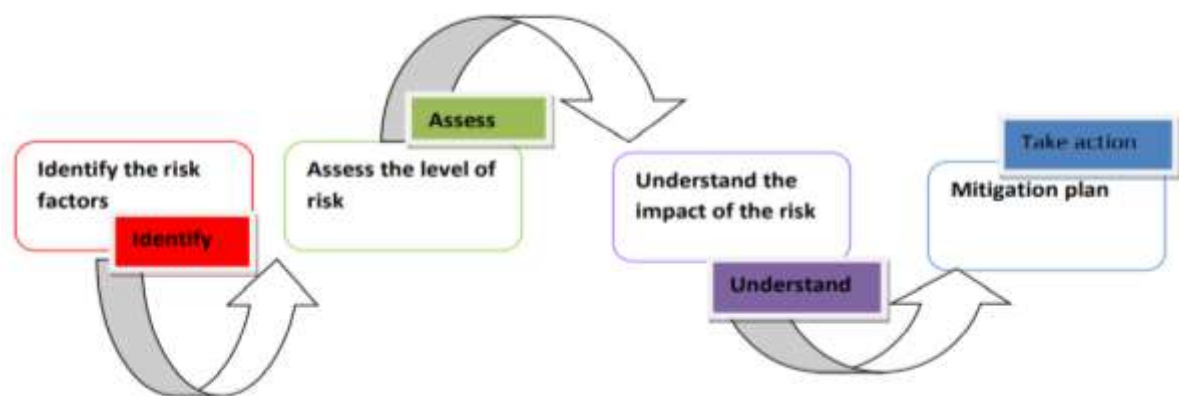


❖ **A vulnerability assessment should analyze the following:**

- Lack of awareness, commitment, knowledge, resources
- Weaknesses/gaps in AML/CFT laws and regulations
- Weaknesses/gaps within Designated Non-Institution and Financial Institutions frameworks (FIU, police, judicial, etc.)
- Weaknesses in infrastructures (ID infrastructure, STR collection and analysis)
- Economic, geographical, or social environment factors
- Low awareness and general or specific control mechanisms.

10.5 Components of the risk-based approach and risk profiling

Our company have taken appropriate steps to identify, assess, understand and mitigate their ML/TF. The assessment should be documented. FATF Recommendation 1 is considered the groundwork towards the implementation of the risk-based approach: See figure below:

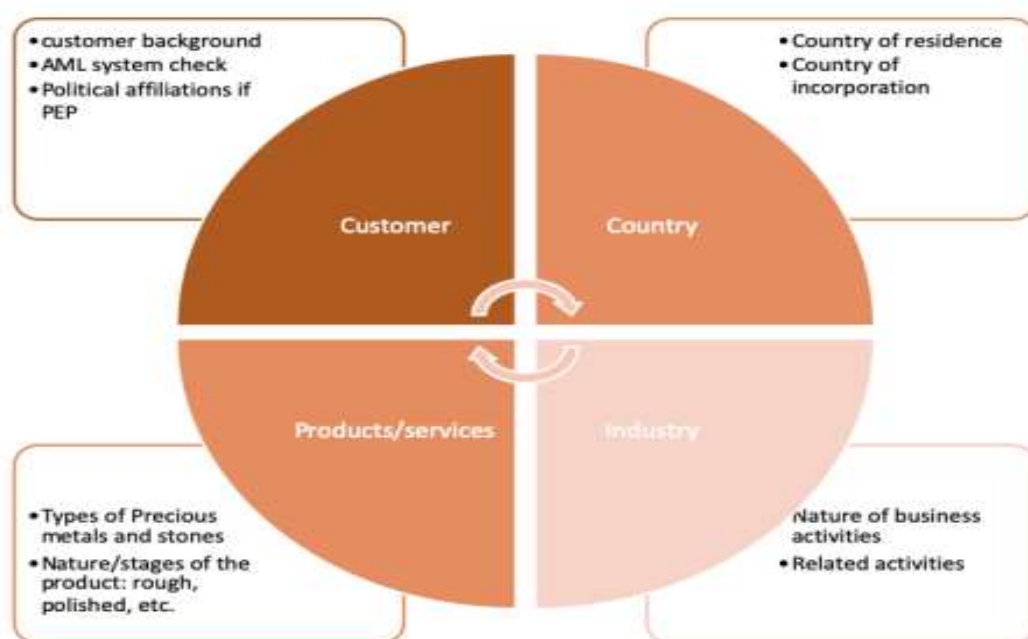


10.6 Risk Factors

Accordingly, the main components that drive a risk assessment by the Designated Non-financial institution are as recommended by the Wolfsberg risk-based approach guidance has provided an insight on the approach by identifying these components that can assist in measuring the risk.

“Money laundering risks may be measured using various categories, which may be modified by risk variables. The most commonly used risk criteria are as follows:

- Country/Geographical risk
- Customer risk
- Product / Transaction and Services risk
- Delivery Channel risk



10.7 Risk Factors for the Precious Metals and Stones Sector

The risk factors have been modified as seen below for the precious metals and stones sector for the purpose of conducting a risk-based assessment in the sector. The list is non exhaustive.

- ❖ **Customer Risk:** Customer risk' in the present context refers to the money laundering risk associated with a particular customer from a Compliance perspective. This risk is based on the risk perceptions associated with the parameters comprising a customer's profile, and the risk associated with the product and channel being used by him.

Customer Type of ESTEEM BULLION FZCO: Table Attached:

Customer Type	Risk Category
Non – Resident	High
Resident	Low*
Corporates	High

*Note: The resident customer risk will be overridden based on the nationality risk.

❖ Product Risk

- Factors that may determine that a customer poses a higher risk include the list below, which is not exhaustive and may also consider other factors.
- Cross border services providing extra anonymity, including Correspondent or international private banking Banknotes or precious metal trading.



- Transactions involving third parties, or outsourcing involve higher risks since there are more ways for money launderers to structure the transfer of money, eventually hiding the party that benefits.
- Customer deals in general trading or occupying general trading license

❖ **Jurisdictional or Country Risk:**

Refers to the money laundering and terrorist financing risks stemming from the country or origin or destination of the funds, or the geographical location of the customer or his business. EDD must always be applied when the:

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

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

❖ **Delivery Channel or Interface Risk:**

A delivery channel is a medium that can be used to obtain a product or service, or through which transactions can be conducted. Delivery channels should be considered as part of the risk of the transactions.

11. Risk Factors of Specific Concern to Dealers in Precious Metals/Stones

The AML-CFT Decision specifies certain risk factors that should be taken into consideration by the company when identifying and assessing ML/FT risk at both the enterprise and the customer levels.

In addition to these organization risk factors, there are a number of additional risk factors which company is aware of and should take into consideration in identifying and assessing the ML/FT risks to which they are exposed. Some of these risk factors depend on the specific stage of the PMS supply chain, and the role of the dealer in regard to the business relationships associated with each stage. Other risk factors relate to the nature and type of the customer or transaction involved.



11.1 Stage of PMS Supply Chain & Role of DPMS

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

- **Extraction/production**

In this stage, the raw minerals containing the PMS are extracted, whether through mechanised industrial means (as in underground or open pit mining) or through artisanal methods (as in alluvial manual collection). This stage may also include the sorting and grading of raw minerals, and their preparation for sale. Key ML/FT risks at this stage include but are not limited to the infiltration of the extraction/production process by criminal or terrorist organisations; vulnerability of the supply chain to the introduction of illicit PMS, or “commingling”; over-, under-, or false invoicing and accounting fraud. ⁸ This stage is also vulnerable to numerous predicate offences, such as theft, embezzlement, smuggling, and bribery/corruption. Thus, the extraction/production process may be used as a vehicle for both the creation of and the laundering of illicit proceeds.

- **Trading in raw minerals**

In this stage, raw ores or rough gemstones are obtained from the extraction source and traded by dealers. This stage of the supply chain may also involve the export and import of raw ores or rough gemstones. Moreover, the market for different types of raw PMS may have different characteristics and regulatory regimes.

For example, the trade in rough diamonds is strongly impacted by the requirements of the Kimberley Process Certification Scheme (KPCS) ⁹, as well as the fact that a significant portion of the international trade is conducted through a group of regulated bourses.

DPMS may participate in this stage of the supply chain as traders of raw materials, either as importers, exporters, or as wholesalers or intermediaries in transactions between other physical or legal persons. Such transactions may take place on a direct party-to-counterparty basis, through tenders or auctions, or via electronic or internet exchanges.

This stage of the PMS supply chain can be one of the most vulnerable to ML/FT risks, in that the number and variety of participants (including street vendors and regional dealers) can be high, and raw minerals may pass through numerous traders’ hands before moving on to the next stage of the supply chain.



Moreover, in the case of some categories of PMS, operational, accounting, and fiscal controls can often be decentralized over multiple geographic regions and legal jurisdictions, making them vulnerable to exploitation by fraudsters, criminals, and terrorists. Key ML/FT risks include but are not limited to:

- ❖ Commingling or entry of conflict minerals into the supply chain, benefitting criminal or terrorist organisations (through falsification of Kimberley Process certifications, in the case of rough diamonds, or smuggling and illegal placing into the market of products from non-participating countries; and due to the absence of international controls equivalent to the KPCS in the case of other PMS);
- ❖ Infiltration of criminal or terrorist organisations among raw mineral traders;
- ❖ Prevalence of cash (or cash equivalent) transactions;
- ❖ Vulnerability to smuggling.

● **Beneficiation**

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

Key ML/FT risks at this stage include but are not limited to: the obscuring of traceability of PMS through the beneficiation process; trade-based ML; the prevalence of cash/cash equivalent transactions; and vulnerability to commingling.

● **Wholesale trade**

In this stage, processed PMS (either refined precious metals or cut and polished precious stones), as well as finished goods (i.e. organization) are traded on a wholesale basis for a variety of purposes, and through diverse channels, some of which may entail the physical exchange of goods and others of which may be virtual in nature (for example, through certificates or various derivative products). These purposes may include but are not limited to transactions involving:

- Sales to manufacturers/fabricators (e.g. jewellers, factories) for use in various finished products or industrial processes;
- Sales to/from other wholesaler dealers/intermediaries or retail merchants for inventory, stockpiling, or speculation/trading;
- Sales related to FIs or commodity exchanges for trading or investment purposes.



DPMS may participate in this stage of the supply chain as wholesale traders or intermediaries, as well as agents/buyers/sellers on behalf of industrial and retail end users.

Key ML/FT risks at this stage include but are not limited to commingling, trade-based ML, and other known typologies and methods associated with placement, layering and integration.

- **Retail trade**

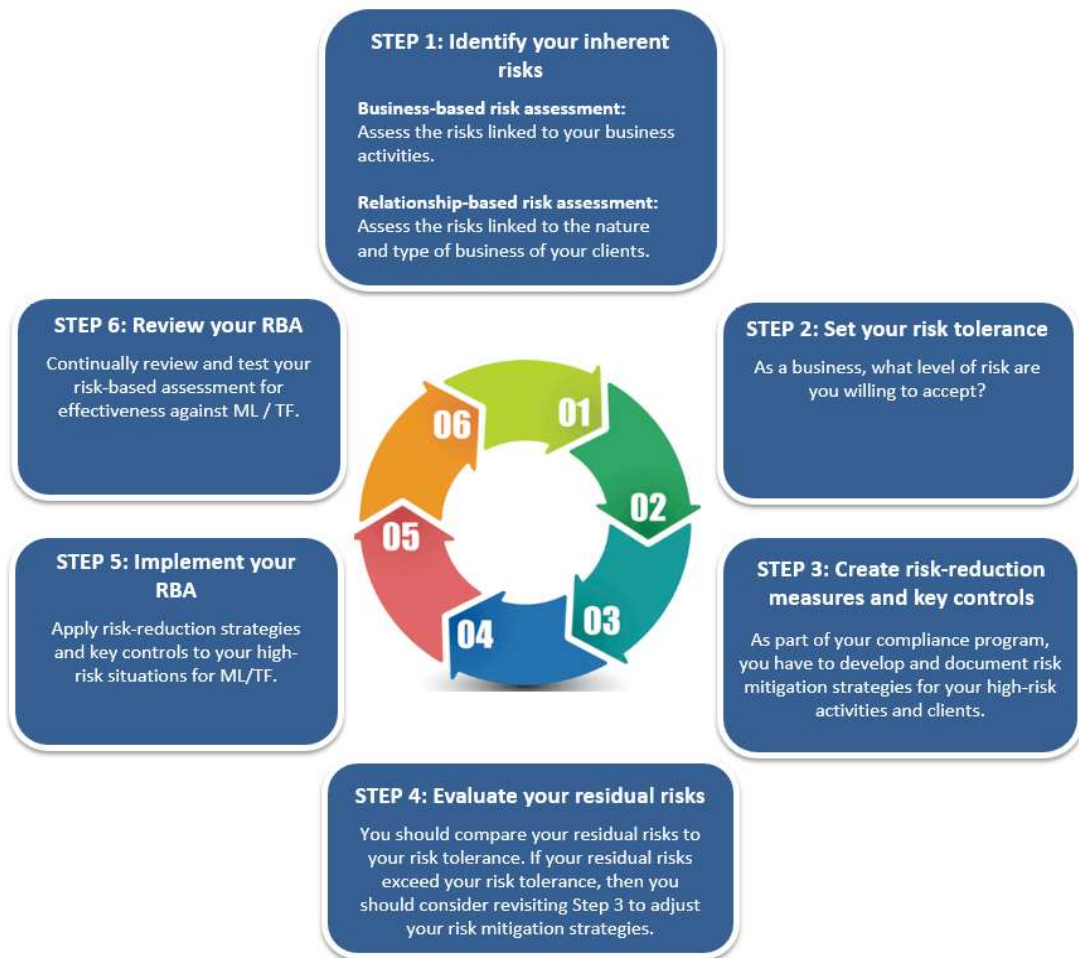
In this stage, beneficiated PMS or finished goods (in particular Jewellery fabricated from PMS) are sold to, or acquired from, retail customers in the primary or secondary markets. DPMS involved in this stage are usually retail merchants involved in selling or buying direct to/from the public. This stage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

12. Enterprise Risk Assessment

can allow supervised institutions to identify gaps and opportunities for improvement in their framework of internal AML/CFT policies, procedures and controls, as well as to make informed management decisions about risk appetite, allocation of AML/CFT resources, and ML/FT risk-mitigation strategies that are appropriately aligned with residual risks.



12.1 Conducting an enterprise risk assessment, as required by Article 4.1 of AML-CFT Decision



ESTEEM BULLION FZCO should decide on both the frequency and methodology of enterprise-level ML/FT risk assessments, including baseline and follow-up assessments, that are appropriate to their particular circumstances, taking into consideration the nature of the inherent and residual ML/FT risks to which they are exposed, as well as the results of the NRA.

ESTEEM BULLION FZCO also decide on policies and procedures related to the periodic review of their enterprise risk assessment methodology, taking into consideration changes in internal or external factors. These decisions will be documented, approved by senior management, and communicated to the appropriate levels of the Organization.



13. National Risk Assessment Summary

The National Risk Assessment (NRA) is an activity undertaken to develop risk-based anti-money laundering and countering the financing of terrorism (AML/CFT) actions and facilitate allocation of available resources to control, mitigate, and eliminate risks.

The NRA will help the company to have a more comprehensive and shared understanding of the inherent risks of Money Laundering and Terrorist Financing faced by the exchange while conducting its business activities.

As part of the NRA, 21 predicate offences have been identified. The NRA at will evaluate its business activities and transactions based on these 21 predicate offenses which are regarded for Money Laundering as defined in the FATF guideline:

- Participation in an organized criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Corruption and bribery
- Fraud
- Counterfeiting and piracy of products
- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint and hostage-taking
- Robbery or theft
- Smuggling (including in relation to customs and excise duties and taxes)
- Tax crimes (related to direct taxes and indirect taxes)
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation.

Monthly data shall be reviewed as per the above national wide offenses to identify risk categorizing by Customer-wise, Transaction-wise, Ultimate Beneficiary wise, Source Identification wise, Supervisory Body Controls and Regulation, Customers Country Financial System, Product and Services offered to Customer, Correspondent/Agent Banking involved and Delivery Channels.

The data shall be analyzed and evaluated based on the finding obtained In the above model to identify and evaluate potential national wide risk for ESTEEM BULLION FZCO. Preventive measure and controls shall be applied in order to mitigate the highlighted risks as identified in the NRA model. EDD shall be conducted on monthly basis for Individual customers and Corporate Customers identified in the model.



14. AML/CFT risk categories handling

- **Prohibited:** ESTEEM BULLION FZCO will not conduct any transactions or dealings of with countries subject to economic sanctions or designated as state sponsors of terrorism, such as those on the United Nations or Office of Foreign Assets Control lists.
- **High-risk:** The risks here are significant, but are not necessarily prohibited. To mitigate the heightened risk presented, the ESTEEM BULLION FZCO applies more stringent controls to reduce the ML/FT risk, such as conducting enhanced due diligence and more rigorous transaction monitoring. Countries that maintain a reputation for corruption or drug trafficking are generally considered high-risk. High-risk customers may include politically exposed persons (PEPs), DNFB- Dealers in precious metals and stones, cash-intensive businesses, general trading and trading companies to name the few.

15. Know-Your-Customer (KYC)

- a. ESTEEM BULLION FZCO maintains clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher risk than average risk. Before accepting a potential client, KYC and due diligence procedure are followed, by examining factors such as customers' background, country of origin, public or high-profile position, linked accounts, business activities or other risk indicators.
- b. KYC is to be carried out according to mandatory Customer KYC checklist as provided for in the Appendix A for
 - (i) Individual shareholders / directors / manager KYC checklist and;
 - (ii) Corporate KYC checklist.
- c. ESTEEM BULLION FZCO is strictly forbidden to transact business with shell companies. Shell companies are institution that has no physical presence in any country, no active business and which merely exists on paper.
- d. An integral part of KYC process is the carrying out of applicant screening and background checking and risk assessment. Applicant screening is designed to ensure that an applicant is not listed on an international official sanction lists issued by government and departments and law enforcement agencies. Background checking is designed to identify any adverse information about the past conduct of an individual that may influence their suitability as an applicant. The risk assessment process clarifies the applicants into three risk categories: low, medium and high.
- e. Extensive due diligence is essential for an individual with high net worth but whose source of funds is unclear. A decision to enter into business relationships with high-risk customers, such as politically exposed persons, is taken exclusively at senior management level.



- f. When conducting the KYC process, there shall be no reliance on third party information or “hearsay”. For applicants introduced to ESTEEM BULLION FZCO by a third party, ESTEEM BULLION FZCO compliance unit must carry out and perform all identification, verification and KYC procedures.
- g. Know Your Customer (KYC) procedures are a critical function to assess customer risk and a legal requirement to comply with Anti-Money Laundering (AML) laws. Effective KYC involves knowing a customer’s identity, their financial activities and the risk they pose.
- h. ESTEEM BULLION FZCO shall see to it that their respective the KYC is a fundamental practice to protect company organization from fraud and losses resulting from illegal funds and transactions.

“KYC” refers to the steps taken by our company as following:

- Establish customer identity
- Understand the nature of the customer’s activities (primary goal is to satisfy that the source of the customer’s funds is legitimate). Assess money laundering risks associated with that customer for purposes of monitoring the customer’s activities.

15.1 Updating Of KYC Information

Know-Your-Customer is an ongoing process. The foundation of any customer due diligence and monitoring procedures lies in the initial collection of KYC information and the ongoing updating of that information. By keeping accurate and up-to-date clients’ records, ESTEEM BULLION FZCO not only manages the risk but also reassures the clients that ESTEEM BULLION FZCO cares about them. Reasonable steps must be undertaken to ensure that KYC information and documents is updated as and when required. As a minimum standard, KYC information must be updated every year.

15.2 Monitoring Of Clients’ Activities

ESTEEM BULLION FZCO is mandated to monitor, supervise and inspect the activities of its clients and their affiliates. As such, the Client Activity Monitoring will be undertaken to

- Collect and retain members’ annual Audited Financial Statements;
- Reviewing the clients’ annual Audited Financial Statements; and
- Conduct inspections of clients’ premises to ensure that their operations are conducted in accordance with UAE Regulatory System.



15.3 Customer Acceptance Policy

ESTEEM BULLION FZCO has clear customer acceptance policy based on applicable rules, regulations and procedures to implement controls for avoiding business relations with any countries and nationalities under sanctions or other criminal offences.

ESTEEM BULLION FZCO staff is responsible to conduct due diligence of any person applying to do business; therefore staff shall obtain satisfactory evidence of the identity and legal existence of persons conducting transactions on the basis of reliable independent documents and record that customer details and other relevant information to the core system and ensure to keep files documents.

Customer Acceptance Policy guidelines are below:

- ❖ Physically examine customer ID Document.
- ❖ Verify ID document and ensure same person is available for service.
- ❖ Take reasonable steps to ensure that identification document is genuine.
- ❖ Update existing customer's records
- ❖ Verify customer's source of income and wealth based on customer profile.

The Customer Identification process as described as below:

The procedures and controls are as follows:

- ❖ Know-your-Customer (KYC) measures.
- ❖ Due Diligence Measures.
- ❖ On-boarding process for legal entities.
- ❖ Sanction and PEP/PEP Screening.
- ❖ Automated Transaction Monitoring.

15.4 KYC Process has 3 stages:

Registration

What is the process of registering customer?

Identification

What does the customer tell you?

Verification

What the customer tells you are correct?



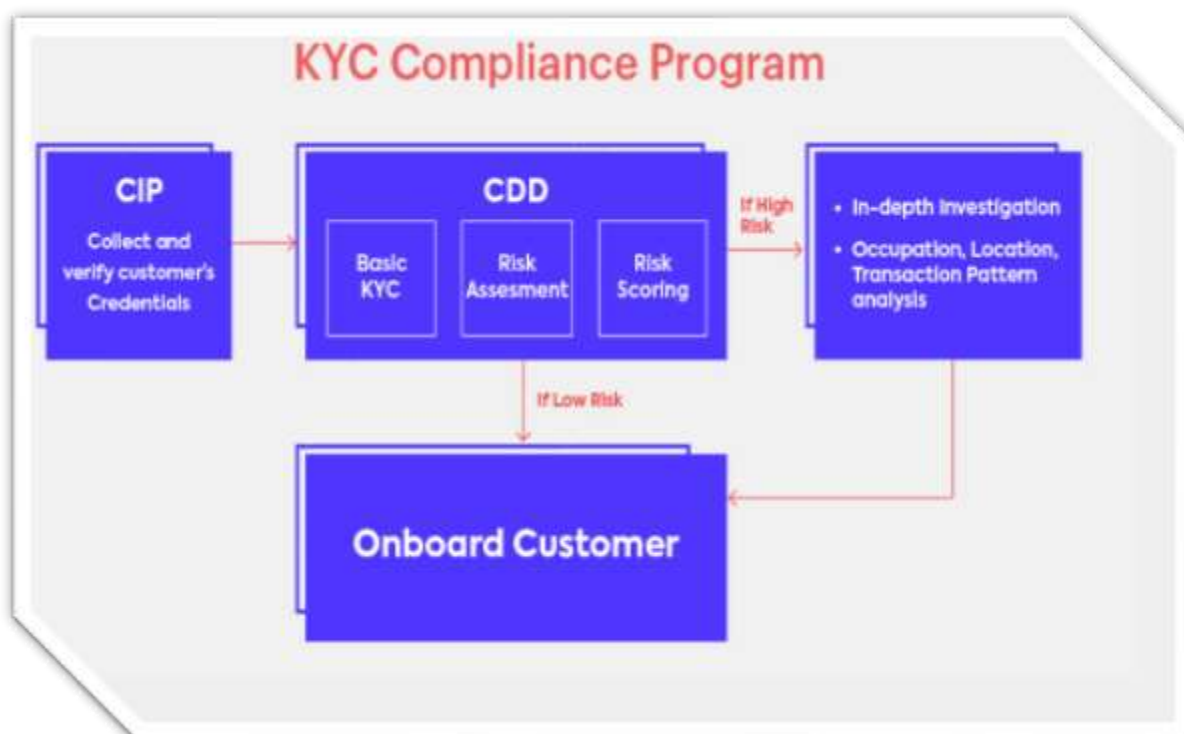
16. Know Your Customer” Procedures and Control

Such measures may include the following:

- Referral of names and other identifying information to criminal investigating authorities; and
- Review of disciplinary history and disclosure of past relevant sanctions.
- i. The Customer Identification Program must include procedures for responding to circumstances in which the Compliance Unit cannot form a reasonable belief that it knows the true identity of a customer.

These procedures should describe, among others, the following:

- When ESTEEM BULLION FZCO should not open an account.
- The terms under which a customer may conduct business transactions while ESTEEM BULLION FZCO attempt to verify the customer’s identity.
- When ESTEEM BULLION FZCO should close an account after attempts to verify customer’s identity fail.
- When ESTEEM BULLION FZCOC should file a Suspicious Transaction Report.
- ii. The Customer Identification Program must include procedures for providing customers adequate notice that ESTEEM BULLION FZCO is requesting information to verify their identities.
- iii. ESTEEM BULLION FZCO shall maintain customer accounts only in the name of the account holder. It shall not open or keep anonymous accounts, fictitious names accounts, incorrect name accounts and similar accounts.
- iv. ESTEEM BULLION FZCO shall ensure that they know their customers well, and accordingly, shall keep current and accurate all material information with respect to their customers by regularly conducting verification and update thereof.



16.1 Identification (ID), Verification (VR) and Know-Your-Customer (KYC)

Documents and information about the customer are verified against independent sources and checked for correctness. Depending on the risks associated with each client or transaction, we apply the appropriate KYC process to each customer. Identification Customer ID verification must be based on a risk-based approach and on the client profile.

However, that the application of a risk-based approach to CDD measures is not to be taken as a static formula by which, for example, all medium-risk customers are necessarily always subjected to normal CDD measures, and all low-risk customers are always subjected to SDD measures. 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, and the appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified. In that regard, supervised institutions should always be prepared to increase the type and level of due diligence exercised on a customer of any ML/FT risk category whenever the circumstances require, including situations in which there are any doubts as to the accuracy or appropriateness of the customer's originally designated ML/FT risk category.



16.2 Circumstances and Timing for Undertaking CDD Measures

Under normal circumstances, ESTEEM BULLION FZCO are obliged to undertake CDD measures (including verifying the identity of customers and Beneficial Owners, beneficiaries, or controlling persons) 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. Guidance in regard to these requirements and certain exceptional circumstances provided for in the AML-CFT Decision is provided in the sub-sections below.

16.3 Establishment of a Business Relationship

ESTEEM BULLION FZCO establish a Business Relationship with a customer when they perform any act for, on behalf of, or at the direction or request of the customer, with the anticipation that it will be of an ongoing or recurring nature, whether permanent or temporary. Such acts may include, but are not limited to:

- Assigning an account number or opening an account (including fiduciary or escrow accounts, and managed accounts held with Financial Institutions) in the customer's name;
- Effecting any transaction in the customer's name or on their behalf, or at the customer's direction or request for the benefit of someone else
- Providing any form of tangible or intangible product or service (including but not limited to granting credits, guarantees, or other forms of value; buying, selling, or leasing physical goods or property of any kind; giving advice, counsel, information or analysis) to or on behalf of the customer, or at the customer's direction or request for the benefit of someone else;
- Signing any form of contract, agreement, letter of intent, memorandum of understanding, or other document with the customer in relation to the performance of a transaction or series of transactions, or to the provision of any form of tangible or intangible product or service as described above;
- Accepting any form of compensation or remuneration (including but not limited to a deposit, retainer fee, or other form of credit or promise of future payment) for the provision of tangible or intangible products or services, as described above, from or on behalf of the customer;
- Receiving funds or proceeds of any kind (including those held on a fiduciary basis, for safekeeping, or in escrow) from or on behalf of the customer, whether for their account or for the benefit of someone else;
- Any other act performed by supervised institutions in the course of conducting their ordinary business, when done on behalf of, or at the request or direction of, a customer.



16.4 Occasional Transactions

During the course of business, Senior Management may be called upon to perform occasional or non-recurring transactions for customers with whom there is no ongoing account or Business Relationship. Examples of such transactions include, but are not limited to:

- Sale or purchase of goods such as precious stones, metals, coins or other valuable property to or from a retail customer;
- Drafting of a Will, Trust agreement, or other legal agreement for a walk-in customer.

On such occasions, and other than in the exceptional circumstances described company will identify the customer and verify the customer's identity (as well as that of the Beneficial Owners, beneficiaries, or controlling persons). Furthermore, company will undertake appropriate risk-based CDD measures including among other things understanding the nature of the customer's business and the purpose of the transaction.

- When carrying out occasional transactions in favor of a Customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
- When there is a suspicion of a crime (see below Identification of Suspicious Transactions);
- When there are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

Some of the indicators of transactions that may appear to be linked include, but are not limited to the following:

- Multiple transactions with the same or similar customer reference codes;
- Transactions executed sequentially or in close time proximity, and involving the same or related counterparties;
- Multiple transactions attempted by a customer with whom there is no Business Relationship at different branches of the same DNFBP on the same day.

16.5 Exceptional Circumstances

From time to time, certain situations may arise which fall outside of the normal course of CDD procedural guidelines. Under these circumstances, described below, our company are permitted to handle the timing, customer identification, and other aspects of customer due diligence procedures exceptionally. Specifically:

- When there is no suspicion of criminal activity, and the ML/FT risks are identified as low, supervised institutions may complete the verification of the customer's identity after establishing the Business Relationship under the conditions specified in the relevant provisions of the AML-CFT Decision.



- Our Company verify the identity of the beneficiaries at the time of settlement or pay-out and prior to the exercise of any related legally acquired rights. We also ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefitting from the Business Relationship prior to the completion of the verification process.
- When our company suspect that a customer or Beneficial Owner is involved in the commitment of a crime related to money laundering, the financing of terrorism, or the financing of illegal organisations, and they have reasonable grounds to believe that undertaking customer due diligence measures would tip off the customer, then we do not apply CDD procedures, but instead we report their suspicion to the FIU along with the reasons that prevented them from carrying out CDD measures.

16.6 Customer Due Diligence (CDD) Measures

The application of risk-based CDD measures is comprised of several components, in keeping with the customer's ML/FT risk classification and the specific risk indicators that are identified. Generally, these components include, but are not limited to, the following categories:

- Identification of the customer, Beneficial Owners, beneficiaries, or controlling persons; and the verification of the identity on the basis of documents, data or information from reliable and independent sources
- Background screening of the customer, Beneficial Owners, beneficiaries, or controlling persons, to screen for the applicability of targeted or other international financial sanctions, and, particularly in higher risk situations, to identify any potentially adverse information such as criminal history.
- Obtaining an understanding of the intended purpose and nature of the Business Relationship, as well as, in the case of legal persons or arrangements, of the nature of the customer's business and its ownership and control structure.
- Monitoring and supervision of the Business Relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behavior.

In cases involving higher levels of risk, our company generally exercise to enhanced levels of customer due diligence, such as identifying and/or verifying the customer's source of funds and taking other appropriate risk-mitigation measures.

- As part of their overall AML/CFT framework, ESTEEM BULLION FZCO consider using a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of CDD procedures. Examples of the some of the factors they should consider include but are not limited to:
 - Procedures and methodologies they implement in analysing and assessing the ML/FT risk of Business Relationships and in assigning appropriate risk classifications;
 - Circumstances, timing, and composition in regard to the application of CDD measures;
 - Frequency of reviews and updates in relation to CDD information;
 - Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which CDD measures are applied.



16.7 Customer and Beneficial Owner Identification/Verification

Grounded on the principles of “Know Your Customer” and risk-based customer due diligence, the identification and ID-verification of customers is a fundamental component of an effective ML/FT risk management and mitigation programme.

The specific requirements concerning the timing, extent, and methods of identifying and verifying customers and Beneficial Owners depend in part on the type of customer (whether a natural or legal person) and on the level of risk involved. However, the core components of a customer’s identification generally remain the same in all cases. They 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 or arrangement); and
- **Principal address**, including evidence of the permanent residential address of a natural person, or the registered address of a legal person or arrangement.
- The verification of a customer’s identity, including their address, should be based on original, official (i.e. government-issued) documents whenever possible.
- In addition to name, nationality, and place of birth, a natural person’s date of birth and national identification number (or the date of establishment and registration number in the case of a legal person or arrangement) are also important elements comprising a customer’s identification, which should be taken into consideration.
- When verifying the identity of foreign nationals associated with high-risk factors, ESTEEM BULLION FZCO should consider validating the authenticity of customer identification documents obtained. Some of the methods that supervised institutions may consider in order to do so, commensurate with the nature and size of their businesses, include but are not limited to
 - ✚ 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
- The types of address verification that may generally be considered acceptable include, but are not limited to, the following categories of documents issued in the name of the customer
 - ✚ Bills or account statements from public utilities, including electricity, water, gas, or telephone 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 insurance policies.



- In addition to the identifying and verifying customers, Beneficial Owners, beneficiaries, and controlling persons, DNFBPs should verify the identity of any person legally empowered to act or transact business on behalf of the customer, whether the customer is a legal or natural person. Such persons may include, but are not limited to:
 - ✚ Signatories, or other persons with authorised remote access credentials to an account, such as internet or phone banking users;
 - ✚ Parents or legal guardians of a minor child, or legal guardians of a physically or mentally disabled or incapacitated person;
 - ✚ Attorneys or other legal representatives, including liquidators or official receivers of a legal person or arrangement
- When verifying that a person purporting to act on behalf of a customer is so authorised, the following types of documents may generally be considered to be acceptable:
 - ✚ 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 authorised legal representative;
 - ✚ A court order or other official decision.
- Whenever possible, and commensurate with the nature and size of their businesses, ESTEEM BULLION FZCO should consider the feasibility of incorporating the “four-eye” principle (review by at least two people) into their procedures with regard to the verification of customer identification documentation and information, as well as with regard to the entry of the relevant data into their information systems.

16.8 CDD Measures Concerning Legal Persons and Arrangements

- Without prejudice to the provisions of Article 9.1(b) of the AML-CFT Decision, when customers that are legal persons are owned or controlled by other legal persons or Legal Arrangements supervised institutions should make reasonable efforts to identify and verify the Beneficial Owners by looking through each layer of legal persons or Legal Arrangements until the natural persons with owning or controlling interests of 25% or more in aggregate are identified.
- When undertaking CDD measures on Legal Arrangements which allow funds or other forms of assets to be added or contributed to the arrangement after the initial settlement and by any persons other than the identified settlor(s), our company will take the necessary steps to ascertain and verify the identity of such persons, and to understand the nature of their relationship with the Legal Arrangement, its settlor(s) and its beneficiaries.



- The AML-CFT Decision obliges trustees in Legal Arrangements to maintain basic information relating to intermediaries, who are subject to supervision, and service providers, including consultants, investors or investment advisors, directors, accountants and tax advisors, who have responsibilities in relation to its management.

16.9 Establishing a Customer Due Diligence Profile

When dealing with higher-risk or more complex customers, in addition to the type of information referred to above, our company consider obtaining and including in the CDD profile more detailed information about their customers' activities, such as (but not limited to):

- Anticipated size and/or turnover of account balances or transactional activity;
- Expected types and volumes of transactions;
- Known or expected counterparties or third-party intermediaries with whom the customer conducts transactions;
- Known or expected locations related to transactional activity;
- Anticipating timing or seasonality of transactional activity.

Where lower-risk customers are concerned ESTEEM BULLION FZCO consider applying more generic due-diligence profiles in order to compare actual and expected types and levels of activity.

Company considers obtaining and including in the profile a detailed explanation or diagrammatical chart showing the entity's internal management structure, identifying the persons holding senior management positions, or other positions of control.

16.10 Ongoing Monitoring of the Business Relationship

In keeping with the level of risk involved, company consider obtaining sufficient information on the counterparties and/or other parties involved (including but not limited to information from public sources, such as internet searches), in order to determine whether the transactions appear to be:

- Normal (consideration should be given as to whether the transactions are typical for the customer, for the other parties involved, and for similar types of customers);
- Reasonable (consideration should be given as to whether the transactions have a clear rationale and are compatible with the types of activities that the customer and the counterparties are usually engaged in);
- Legitimate (consideration should be given as to whether the customer and the counterparties are permitted to engage in such transactions, such as when specific licenses, permits, or official authorisations are required).



Some of the methods that may be employed for the 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 a certain type are examined;
- Location-based rules, in which a certain percentage (or even all) of the transactions involving a specific 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.

Furthermore, monitoring procedures may be automated, semi-automated, or manual, depending on the nature and size of their businesses. Whichever methods they elect to use, however, supervised institutions should consider documenting them, obtaining senior management approval for them, and periodically reviewing and updating them to ensure their effectiveness. Company also consider establishing specific monitoring procedures for customers and business relationships which have been reported as suspicious to the FIU.

16.11 Reviewing and Updating the Customer Due Diligence Information

The timely review and update of customer due-diligence information is a fundamental component of an effective ML/FT risk management and mitigation programme.

The company maintains the due-diligence documents, data and information obtained on customers, and on their Beneficial Owners or beneficiaries in the case of legal persons or arrangements, up to date.

- **Circumstances, timing and frequency:** to establishing clear rules with respect to circumstances that would trigger an interim or special review, or the acceleration of a particular customer's review cycle. Such circumstances might include, but are not necessarily limited to:
 - ✚ Discovery of information about a customer that is either contradictory or otherwise puts in doubt the appropriateness of the customer's existing risk classification or the accuracy of previously gathered due-diligence data.
 - ✚ Expiry of a customer's or Beneficial Owner's identification documents.
 - ✚ Material changes in ownership, legal structure, or other relevant data (such as name, registered address, purpose, capital structure) of a legal person or arrangement.
 - ✚ Initiation of legal or judicial proceedings against a customer or Beneficial Owner.
 - ✚ Finding materially adverse information about a customer or Beneficial Owner, such as media reports about allegations or investigations of fraud, corruption, or other crimes.
 - ✚ Qualified opinion from an independent auditor on the financial statements of a legal entity customer.
 - ✚ Transactions that indicate potentially unusual or suspicious patterns of activity.



- **Components and extent:** establishing protocols with regard to the extent of the review and examination of due-diligence information for Business Relationships in different risk categories. Examples of such protocols might include, but are not necessarily limited to:
 - ✚ When the source of wealth/funds of a customer should be verified.
 - ✚ When additional inquiries or investigations should be made pertaining to the nature of a customer's business, the purpose of a Business Relationship, or the reasons for a transaction.
 - ✚ How much of a customer's transactional history, including how many and which specific transactions or transaction types, should be reviewed as part of a regular periodic or an interim review.
- **Organizational roles and responsibilities:** consider clearly defining the relevant organizational arrangements in relation to the customer due-diligence review/update process. Examples of such roles and responsibilities might include, but are not necessarily limited to:
 - ✚ Carrying out reviews/updates
 - ✚ Escalating and/or reporting situations in which risk classifications should be changed, Business Relationships should be suspended or terminated, or unusual or potentially suspicious activities should be further investigated
 - ✚ Approving or rejecting reviews of Business Relationships (including senior management involvement with regard to PEPs and other High-Risk Customers).
 - ✚ Undertaking CDD file remediation measures as may be necessary.
 - ✚ Auditing the quality of customer due-diligence reviews/updates.
 - ✚ Maintaining records with regard to customer due-diligence reviews/updates, in accordance with statutory record-keeping requirements.

16.12 Enhanced Due Diligence (EDD) Measures

EDD in cases of identified High Risk Customers, apply it in any situation in which there are doubts about the accuracy or appropriateness of a customer's ML/FT risk classification, or in which there are red-flag indicators of potentially unusual or suspicious activity. In all cases in which EDD is applied, company takes reasonable measures to obtain adequate information about the customer, commensurate with the level of the risks identified.

- Procedures and methodologies they implement in analysing and assessing the ML/FT risk of Business Relationships and in assigning appropriate risk classifications, especially with regard to high-risk categories;
- Circumstances, timing, and composition in regard to the application of EDD measures;
- Frequency of reviews and updates in relation to customer EDD information;
- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which EDD measures are applied.



The results of both the NRA and our own enterprise-wide ML/FT risk assessments is reasonable and proportionate to the risks involved, and, in formulating them. Also our company policies, procedures and methodologies is documented, approved by senior management, and communicated at the appropriate levels of the organisation.

Generally speaking, EDD involves a more rigorous application of customer due diligence measures, including, but not limited to, such elements as:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to customer identity.
- More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions.
- Increased supervision of the Business Relationship, including the requirement for higher levels of management approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.

16.13 EDD Measures for High-Risk Customers or Transactions

To apply EDD measures to manage and mitigate the risks associated with identified High Risk Customers and/or transactions. The AML-CFT Decision defines a High-Risk Customers as including those who represent a risk:

- Either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a customer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party.
- The reason for a foreign customer's or Beneficial Owner's presence, or establishment of a Business Relationship, in the UAE;
- Consistency between the nature of the customer's business and transactions and the customer's or Beneficial Owner's professional background and employment history. may find it helpful to obtain background information from reliable and independent sources, as well as from internet and social media searches, and from the customer's or Beneficial Owner's CV.
- The level of complexity and transparency of the customer's transactions (and/or legal structure, where legal persons or arrangements are concerned), especially in comparison with the customer's or Beneficial Owner's educational and professional background;
- The nature of any other business interests of (including any other legal persons or arrangements owned or controlled by) the customer or Beneficial Owner;
- Consistency between the customer's line of business and that of the counterparty to the customer's transactions (as identified, for example, through internet searches).



Additionally, and commensurate with the nature and size of their businesses, when carrying out EDD measures in respect of High Risk Customers or Beneficial Owners.

- Performing background checks (including but not limited to the use of internet searches, public databases, or subscription information aggregation services) to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information;
- Using more rigorous methods for the verification of the customer's or Beneficial Owner's identity in regard to High Risk Customers.

16.14 Requirements for High-Risk Countries

- The organisation's risk appetite and customer acceptance policies pertaining to Business Relationships involving high-risk countries.
- Methodologies and procedures for assessing and categorising country risk, and identifying high-risk countries (in addition to the statutorily defined High Risk Countries).
- Determination and implementation of appropriate risk-based controls (for example, certain product or service restrictions, transaction limits, or others) with regard to customers and Business Relationships associated with high-risk countries.
- Organisational roles and responsibilities in relation to the monitoring, management reporting, and risk management of high-risk country Business Relationships;
- Appropriate procedures for the enhanced investigation of Business Relationships involving high-risk countries in relation to their assessment for possible PEP associations;
- Independent audit policies in respect of EDD procedures pertaining to customers and Business Relationships involving high-risk countries, and the business units that deal with them.



16.15 Simplified Due Diligence (SDD) Measures

SDD are permitted to exercise simplified customer due diligence measures (SDD) with regard to customers identified as low-risk.

SDD generally involves a more lenient application of certain aspects of customer due diligence measures, including, but not limited to, such elements as:

- A reduction in verification requirements with regard to customer or Beneficial Owner identification
- Fewer and less detailed inquiries in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- More limited supervision of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information.

Specifically, the AML-CFT Decision permits the application of SDD in the following circumstances:

- **Identified low-risk customers:** When the customer or Beneficial Owner is identified as posing a low risk of ML/FT, company permit to complete the verification of their identity after the establishment of a Business Relationship under the conditions specified in the relevant provisions of the AML-CFT Decision.
- Holding funds in suspense or in escrow until the identification verification is completed
- Making the completion of identification verification a condition precedent to the closing of a transaction.
- to establish the Business Relationship prior to the completion of the verification process, which may include (but is not limited to) such steps as: obtaining appropriate supporting documentation, certifications or attestations, when necessary (for example, as regards the corporate documents of a legal person); or obtaining all the necessary information related to the relevant parties of a legal person or Legal Arrangement, such as Beneficial Owners, settlors, trustees or executors, protectors, beneficiaries, or other controlling persons.



- **Listed companies:** exempted from identifying and verifying the identity of any shareholder, partner or Beneficial Owner of a legal person under the conditions specified in the relevant provisions of the AML-CFT Decision. Namely:
 - ✚ When the relevant identity information is obtained from reliable sources; and
 - ✚ When the customer, or the owner holding the controlling interest of the customer, is a company listed on a regulated stock exchange subject to adequate disclosure and transparency requirements related to Beneficial Ownership; or when the customer, or the owner holding the controlling interest of a legal entity customer, is the majority-held subsidiary of such a listed company.
 - ✚ Procedures and methodologies they implement in analysing and assessing the ML/FT risk of Business Relationships and in assigning appropriate risk classifications, especially with regard to low-risk categories;
 - ✚ Circumstances, timing, and composition in regard to the application of SDD measures;
 - ✚ Frequency of reviews and updates in relation to customer SDD information
 - ✚ Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which SDD measures are applied.

16.16 Reliance on a Third Party

- Ensure that the third party is regulated and supervised, and adheres to the CDD measures towards Customers and record-keeping provisions of the present Decision.
- Clearly defined procedures for determining the adequacy of a third-party's CDD measures, 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. (In this regard, supervised institutions are advised that tools such as questionnaires, scorecards, and on-site visits may be useful in evaluating the adequacy of a third party's adherence.)
- Service-level agreements, clearly setting out the roles and responsibilities of the parties and specifying the nature of the CDD and record-keeping requirements to be fulfilled.
- Protocols for the certification by third parties of documents and other records pertaining to the CDD measures undertaken.



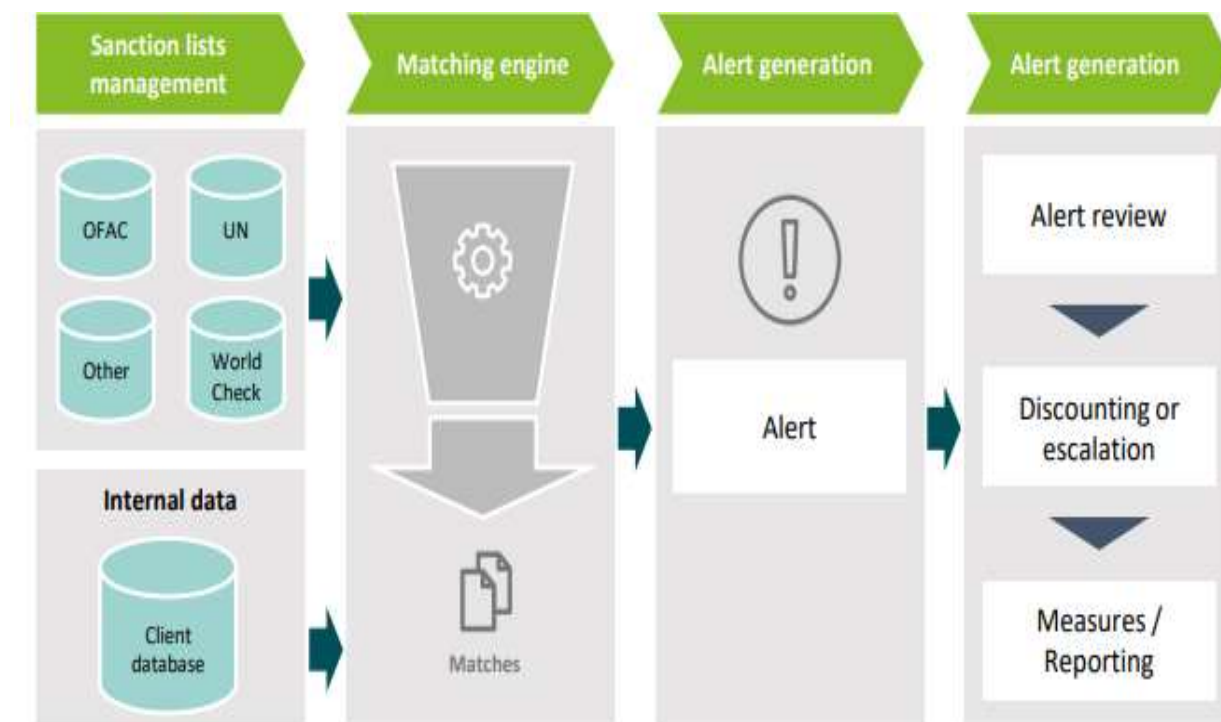
17. Sanctions Screening

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

Our sanctions compliance program is designed to ensure that ESTEEM BULLION FZCO complies with applicable economic sanctions laws in every jurisdiction with which it may choose to trade or operate. A sanctions compliance program includes two types of screening control: transaction screening and customer screening.

Both types of controls are dependent on a reliable matching engine that compares data from internal and external sources against each other, in order to detect similarities that indicate a possible match. Once a possible match has been identified, an alert is generated. It is then routed to a compliance officer for review, to assess whether the alert indicates a 'true match' or is a 'false positive'. On identifying a true match with sufficient confidence, the institution needs to apply the necessary measures such as blocking a transaction and reporting to the relevant authorities.

The sanctions screening process:



An effective data management process has become ever more important for institutions, in order to be able to keep up with the changing sanctions landscape and to remain compliant with their regulatory obligations. In this thought piece we look at the fundamentals of data management and a potential approach to building a robust sanctions screening program.



17.1 Data Management

Data management involves the collection, maintenance, and use of data in a secure, efficient and effective way. Organizations increasingly see data as a key asset for creating value, a robust data management strategy is therefore growing in importance.

“The goal of data management is to help people, organizations, and connected things optimize the use of data within the bounds of policy and regulation so that they can make decisions and take actions that maximize the benefit to the organization”.

A well-maintained data management strategy can help organizations to gain a competitive advantage over their business rivals, as it improves operational effectiveness and decision-making. Organizations that have control over their data can also be more agile, spotting market trends earlier taking proactive measures sooner.

“Treating data as an asset can result in diverse benefits, which can be monetized, measured and managed”.

17.2 The sanctions screening process

Data management consists of several elements.



- **Data Governance:** Data governance refers to the set of guidelines (planning, monitoring and enforcement) for managing data assets and making sure that everyone abides by the rules.
- **Data Architecture:** Data architecture is the conceptual structure or framework of the data management environment, its components and interactions. It “interrelates the framework, people, processes, project policies, technologies and procedures to manage and use valuable enterprise information assets”.
- **Data Integration:** Data integration is the process of bringing together data from various sources/data collection channels, and putting them into a format for processing.



- **Data Privacy:** Data privacy is concerned with the privacy and sensitivity of the personal data about customers, and procedures for ensuring that personal data is collected, shared and used in appropriate ways.
- **Data Quality:** Data quality refers to the accuracy, completeness, timeliness and consistency of data, together with the requirements and rules for its use. Data quality issues are the cause of most data management. “Without data governance, data quality effort becomes a costly one-off exercise”. In order to assure the quality of data, it is necessary to understand its purpose, action, context, and how it is measured.
- **Master Data (Management):** In a business context, master data is the core data within a system. It is not transactional in nature, although it can include records of transactions. It represents an organization’s most valuable data assets. The purpose of master data management is to provide processes for the collection, aggregation, matching and consolidation of data. Master data represents an organizations’ “singlesource-of-truth” for a specific data set and ensures a common understanding.

17.3 The importance of a data management cycle for effective sanctions screening

The Wolfsberg Group principles states: “Sanctions screening is used in the detection, prevention and disruption of financial crime and, in particular, sanctions risk. It compares data sourced from a financial institution’s operations, including as customer and transactional records from structured (KYC) as well as unstructured (product documentation, client notes) sources, against lists of sanctioned names and other indicators of sanctioned parties or locations”.

Since financial institutions process large volumes of client and transaction data on a daily basis, screening this data against relevant sanction lists can be a challenging task. ESTEEM BULLION FZCO are obliged by the regulations to ensure that they will not have a relationship with individuals or entities that are present on the sanction list and neither with entities that are owned by or linked to sanctioned persons and entities. This is not an easy task, as many individuals use similar names, resulting in large amounts of false positives. Peripheral information, such as geographic locations, addresses, occupation, or date of birth may be used to determine the accuracy of a match – data completeness and quality increase the possibility of confirming a true match.

Also obliged to screen high-risk transactions going through customer accounts, in order to ensure that customers do not transfer money to or from sanctioned individuals, entities, jurisdictions or business sectors. Each institution should decide which types of transactions and which attributes within them are relevant for sanctions screening. Beneficiaries and senders of transactions are relevant for list-based sanctions programs, whereas addresses are more relevant for screening against geographical sanctions programs. Other common transactional attributes used for screening include vessels, agents, intermediaries, and free text fields such as payment reference information or the stated purpose of the payment in field 70 of a SWIFT message.



17.4 Sanctions screening data management

Screening controls rely on both internal and external data sources. Some of the key internal data sources across geographical locations and business sectors are master (customer) data, transactional data and other business sector-specific customer information. External data sources include sanctions lists and additional indicators of sanctioned parties. Additional external data sources such as public registers, government lists or other reliable independent licensed sources for data enrichment may also be used for screening.

Data sources are often distributed across multiple IT systems and must be identified in order to be able to assess which elements of data are needed for the screening process. The purpose of data identification is to obtain a holistic view of the institution's customer base.

It is important that all data sources can be linked and integrated at the most granular level possible, and should have the same quality standards.

Before customer, reference or transactional data can be used for screening, it must be extracted, enriched, mapped, transformed and/or loaded into a single platform. If data is corrupted or compromised in the process, sanctions screening model will not operate as intended. The 'Supervisory Guidance on Model Risk Management', issued by the Office of the Comptroller of the Currency (OCC), states: "Process verification includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available". Therefore company ensure that data quality, completeness and integrity is tested, documented and monitored on a regular basis.

17.5 Sanction lists management

While it may seem that sanction lists are simple and straightforward, in practice they involve large amounts of varied data, including not just the names of listed entities and individuals but also additional details such as known abbreviations, acronyms, aliases, and geographic locations. In order to establish an effective management process, institutions should clearly define who is responsible for the delivery and maintenance of sanction lists.

The first step in the sanctions list management process is to determine and prioritize the lists deemed relevant for screening. These may be externally sourced lists from third party list providers or lists from regulatory websites (e.g. OFAC, UN, EU) as well as internal lists of individuals, entities, regions, ports or prohibited goods. The selection of lists depends on various factors such as type of clients, products offered, and nature of the business. In order to select relevant lists, company will complete a risk-based assessment and take into consideration relevant regulatory requirements.

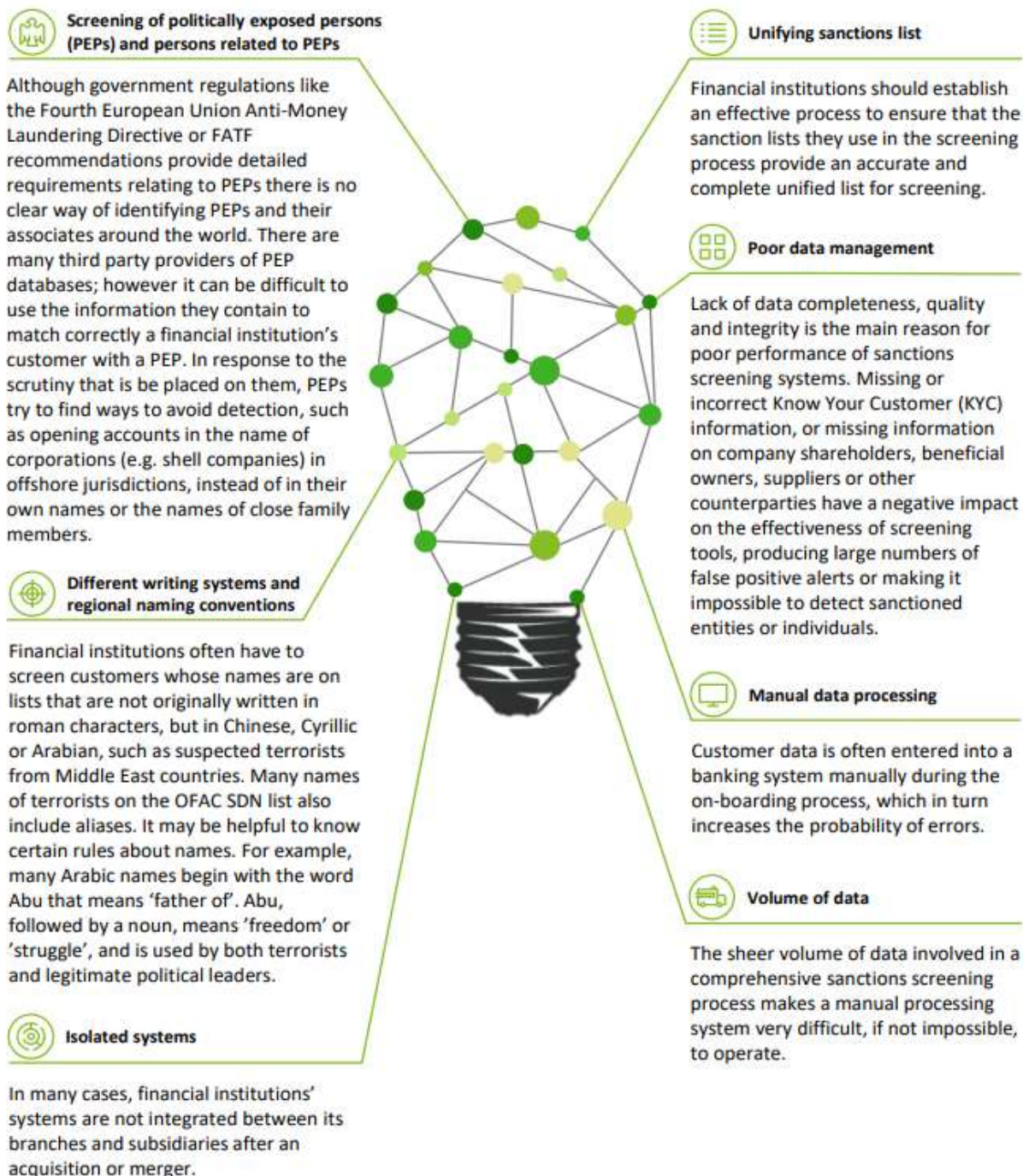
That use external vendors for sourcing and maintaining regulatory sanction lists should have a formal process for reconciling its third party provided lists with regulatory lists, to ensure completeness.

On the other hand, relying solely on sanction lists from regulatory websites must ensure that their process should involve consolidating data from multiple sources, which may be in different formats. In addition, some individuals/entities will be included in more than one list, so it is necessary to remove duplicates as not doing so may cause an alert to be generated twice. In such cases, the company will consider implementing a sanction list management system to clean, parse and format the list data in order to improve matching accuracy and reduce number of false positives.



17.6 Challenges in managing data for sanctions screening

Company may face many challenges to data management for sanctions screening purposes. Here are some examples:





17.7 Potential solution and its benefits

Design and implementation: The figure below illustrates the implementation and operation of a solution for company in establishing an effective sanctions screening process. The solution would need to be partially automated, tailored to specific business needs, and designed with a holistic risk-based approach. The implementation of the solution generally follows a defined process, which consists of the following steps:

The sanctions screening process

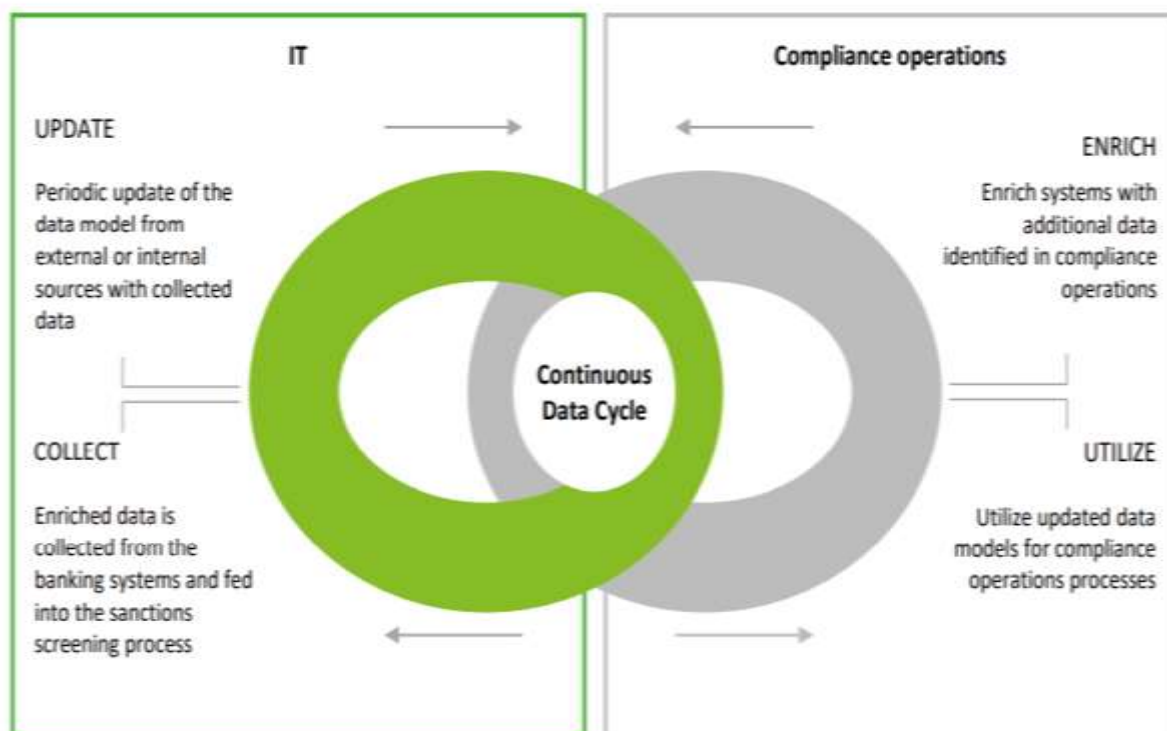


- **Initiation:** A top-down approach is required, in which the relevant stakeholders are involved from the very beginning. Technology and a data-driven approach are required to run an effective sanctions screening process. The organization of the project should be defined beforehand in order to be able to involve the relevant stakeholders throughout all phases of the project.
- **Assessment:** The assessment is based on the business requirements, and addresses associated risks, the quality of the required data and the data architecture, as well as the existing processes that are impacted by the screening system.
- **Design and implementation:** The data model builds the technical foundation for the potential solution. It should be flexible and expandable. Tailored ‘extract, transform, load’ (ETL) processes must ensure that up-to-date data is collected and is transformed appropriately. Integration interfaces allow information to be leveraged by relevant business processes.
- **Go Live:** Before a technology solution goes live, the process governance must be defined and users must be trained. Another crucial aspect is the deployment and maintenance of the solution, e.g. versioning of the solution in the deployment process to ensure streamlined maintenance and ensure that new versions are deployed correctly.



- Design and implementation:** Once it is operating, the system should ensure a continuous cycle of data between the organization's IT systems and the screening system of the compliance department. Data triggered by the sanctions screening process, such as the findings from a related internal investigation or updates to client risk scoring models, should be updated automatically in the respective IT systems. This enables the IT systems to extract accurate data for inclusion in the screening model.

Continuous data cycle for sanctions screening



This diagram shows a framework for a continuous cycle of data management for sanctions screening purposes. Internal data from the organisation's IT systems flow into the screening process, where it is enriched with additional information and then fed back into the IT systems.

To ensure continuity of the process, a data management officer should be appointed to perform an oversight function.

In summary, effective data management and analytics play an important role in detecting and reducing the risk of financial crime. Regulators from all over the world emphasise the importance of implementing new technologies to enhance the sanctions screening programs of financial institutions.



17.8 Sanctions screening trends

With growing data volumes and an ever-changing sanctions screening landscape, the need for automated processing and cataloguing of data as well as real-time sanctions screening will be ‘a must’. Recent trends within large institutions point to the deployment of a more holistic approach and greater use of available data.

“Information sharing is critical for Combating money laundering, terrorist financing and financing of proliferation. Barriers to information sharing may negatively impact the effectiveness of AML/CFT efforts. This underscores the importance of having rapid, meaningful and comprehensive sharing of information.”

A.1. Individual Customers

- a) ESTEEM BULLION FZCO shall obtain from all individual applicants the following information:

Applicant’s full name (as per passport);

- Date and place of birth;
 - Nationality;
 - Physical Address (residential and business / home country and UAE);
 - Contact details;
 - Previous personal / business activities / occupation (type and volume);
 - Anticipated type and volume of company’s activities;
 - Bank reference and introductory letter; and
 - Source of funds.
- i. ESTEEM BULLION FZCO shall request individual applicants who present only photocopies of identifications and other documents to produce or show the original documents for verification purposes. The relevant documents listed in Appendix A hereof shall be obtained in respect of individual applicants.
- ii. Wherever possible, prospective clients should be interviewed personally. AESTEEM BULLION FZCO shall take particular care in opening accounts via the internet, email, post or telephone or other such instances which may give rise to verification without face-to-face contact.
- iii. The customer identification procedures for non-face-to-face verification should be as stringent as those for face-to-face verification. ESTEEM BULLION FZCO is duty-bound to inform such clients that identity verification measures apply as well to them.
- iv. The following are a number of checks which can be used by ESTEEM BULLION FZCO to verify identity of prospective clients where there is no face-to-face contact:



- Telephone contact with the applicant at an independently verified home or business number;
- Subject to the applicant's consent, telephone verification of the applicant's employment with the employer's personnel department at a listed business number;
- Income or salary details appearing on recent bank statements, income tax returns or any other document evidencing income or compensation;
- Confirmation of the address through an exchange of correspondence or by other appropriate methods;

A.2. Corporate Customers

- a) Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In case of doubt as to the veracity of the corporation or identity of its directors and/or officers, or the business or its partners, a search or inquiry with relevant Supervising Authority/Regulatory Agency shall be made.
- b) ESTEEM BULLION FZCO shall obtain from all corporate account applicants the following information. The relevant documents listed in Appendix A hereof shall be obtained in respect of corporate / other business applicants.
 - Incorporated name;
 - Shareholders (in case applicant company being non-publicly traded);
 - Ultimate beneficial owners (in case applicant company is not publicly-traded);
 - Managers;
 - Signatories;
 - Country of origin / UAE physical address (if applicable);
 - Contact details;
 - Previous business activities (type and volume);
 - Anticipated type and volume of activities;
 - Last two years audited financial statements
 - Source of funds; and
- c) Bank reference and introductory letter c. For companies or businesses registered outside the United Arab Emirates, comparable documents are to be obtained, duly authenticated by UAE Embassy where said embassy are located.
- d) If significant changes to the company structure or ownership occur subsequently, or suspicions arise as a result of a change in the payment profile as reflected in a company account, further checks are to be made on the identified of the new owners.



A.3 Know Your Customer (KYC) (Corporate Customer)

1. Company Details	
a. Name	
b. Registered Address	
c. Business Address	
d. Phone Number	
e. Date of Incorporation	
f. Country of Incorporation	
g. Business Registration Number	
h. Tax Identification/Registration number	
i. If listed, indicate name of stock exchange(s) and ticker	
j. Website	
k. How many direct and indirect subsidiaries does the company have?	
2. Business Activity	
a. Type of Business	Bank Jeweller Precious Metals Trader/Dealer Scrap dealer Other Financial Intermediary Coins dealer Industrial Mint Wholesaler Others, please specify:
b. Description of core business activity	
c. Does the company hold a license to conduct its business (yes)? Please provide a copy(yes)	
d. Main Market	
e. Main Products	

**3. Beneficial Owners****SHAREHOLDER(S)**

Percentage Holding (%)	Name	Address	Country of Incorporation/ Nationality	Date of Incorporation/ Date of Birth

4. Ultimate Beneficial Owner

Percentage Holding (%)	Names	Address	Nationality	Date of birth

5. Authorized Signatory List

Name	Passport number	Nationality	Specimen Signature

6. Letter of Authorized

Undertaking for Business transaction: We are hereby authorize the following on behalf of our company and to sign the necessary transaction Vouchers. His/her original identity documents will be produced by him /her at the time of transaction

Name of the Employee	ID Details of the employee	Specimen Signature

7. Management Structure

a. Board of Directors				
b. Management				

8. Bank Details

Account Name	
Bank Address	
IBAN	

9. Contact Person

Name		Designation		E-mail		Phone	
Transaction's confirmations should be sent to following emails							
E-mail 1D							



10. Facilities	YES	NO	N/A
a. Does the Company have any smelting or refining facilities?			
b. Does the Company have any manufacturing facilities?			
c. Does the Company produce its own jewellery?			
d. What are the types, forms and percentage of precious metals sourced by the Company <input type="checkbox"/> Recycled precious metals (%_____) <input type="checkbox"/> LBMA GD Bullion <input type="checkbox"/> Non LBMA Good Delivery Bullion <input type="checkbox"/> Rudimentary Bars <input type="checkbox"/> Jewellery <input type="checkbox"/> Broken jewellery <input type="checkbox"/> Coins <input type="checkbox"/> Collected waste <input type="checkbox"/> Others, please specify: _____ <input type="checkbox"/> Primary material – mined precious metals (%_____)			
e. What type of precious metals is the Company planning to send for refining? <input type="checkbox"/> Gold <input type="checkbox"/> Others, please specify: _____			
f. What is the form of precious metals planned to be sent for refining? <input type="checkbox"/> Unprocessed recycled precious metals <input type="checkbox"/> LBMA GD Bullion <input type="checkbox"/> Non LBMA Good Delivery Bullion (Au =>995 / AG=>9999) <input type="checkbox"/> Coins <input type="checkbox"/> Jewellery <input type="checkbox"/> Broken jewellery <input type="checkbox"/> Own production waste <input type="checkbox"/> Collected waste <input type="checkbox"/> Melted recycled precious metals <input type="checkbox"/> Rudimentary Bars (undefined dimension and fineness) <input type="checkbox"/> Others, please specify: _____			
11. Precious Metals Suppliers Due Diligence Questionnaire	YES	NO	N/A
1. Does the Company perform enhanced due diligence for high risk precious metals supplier			
2. Does the Company assess its corporate precious metals suppliers' AML-CFT and purchase procedures and practices			



12. Transactions monitoring	YES	NO	N/A
Does the Company perform a risk-based assessment to understand the normal and expected transactions of its suppliers (in order to identify the unusual transactions)?			
Does the Company have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments (e.g. traveler's cheques) or third party payments?			
Does the Company have to register all purchases and sales?			

A.4 Attachment – To Be Filled In Only For Company Subject To AML - CFT Regulation

13. Wolfsberg Anti-Money Laundering Questionnaire		
Corporate Name:		
Location:		
If you answer “no” to any question, please ensure that an explanation and additional information is supplied at the end of the relevant section		
I. General AML Policies, Practices and Procedures:	Yes	No
1. Is the AML compliance program approved by the Corporate's board or a senior committee?		
2. Does the Corporate have a legal and regulatory compliance program that includes a designated Compliance officer that is responsible for coordinating and overseeing the AML framework?		
3. Has the Corporate developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions?		
4. In addition to inspections by the government supervisors/regulators, does the corporate client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?		
5. Does the Corporate have a policy prohibiting accounts/relationships with shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group).		
6. Does the Corporate have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?		
7. Does the Corporate have policies covering relationships with politically exposed persons (PEP's), their family and close associates?		
8. Does the Corporate have record retention procedures that comply with applicable law?		
9. Does the Corporate require that its AML policies and practices be applied to all branches and subsidiaries of the corporate both in the home country and in locations outside of the home country?		



14. DOCUMENTS REQUIRED	
Please provide certified copies of the following documents	
1. Business Registration	
2. Certificate of Incorporation	
3. Latest Annual Financial Statements	
4. Cancelled Company Letterhead	
5. 5Proof of Registered Physical Address	
6. Memorandum and Articles of Association (If Applicant is an incorporated company)	
7. VAT Registration Certificate	
8. Board Resolution in respect of trading limits / signing authorities	
9. Permit / Licenses	
10. Bank Details	

Space for additional information (Please indicate which question the information is referring to):

Acknowledgement And Declaration

I/We [the client] hereby acknowledge and declare by our signature to this document that:

I/We am/are aware of and will abide by all local regulatory requirements relating to compliance, anti-money laundering, terrorist financing and dealing in conflict minerals.

I/We am/are not involved or engaged either directly or indirectly with any form of illegal activities relating to the conduct of my metals business with my/our clients or associates or counterparts.

All information provided by me/us in this application is true and accurate.

SIGNATURE

I hereby declare that the information given above is true and accurate as of the date of writing.

	Authorised Signatory	Authorised Signatory
Signature:		
Print Name:		
Title:		
Company Name		
Date and location:		



18. Suspicious Transactions/ Unusual Transactions

ESTEEM BULLION FZCO shall institute a system for the mandatory reporting of suspicious transactions pursuant to Federal Law No. 4 of 2002 regarding criminalization of money laundering. Any transactions settled in cash and which has a value of One Hundred Thousand Dirhams (AED 100,000/-) or above should be accompanied by a certificate of source of funds such as bank cash payment certificate or slip, customs declaration certificate, etc.

Any suspicious transactions must be reported to Anti-Money Laundering and Suspicious Cases Unit (AMLSCU). Where any employee or personnel, director or officer of ESTEEM BULLION FZCO knows that the client has engaged in any of the predicate crimes under the UAE Federal Law, the matter must be promptly reported to the Compliance Officer within the organization who, in turn, must immediately report the details to the AMLSCU.

If there are reasonable grounds to suspect that the customer has engaged in an unlawful activity, the Compliance Officer, on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the AMLSCU unless the compliance officer/s or unit considers, and records an opinion, that such reasonable grounds do not exist.

ESTEEM BULLION FZCO directors, officers, and employees shall not warn their customers that information relating to them has been reported or is in the process of being reported to the AMLSCU, or communicate, directly or indirectly, such information to any person other than the AMLSCU. Any violation of this confidentiality provision shall render them liable for criminal, civil and administrative sanctions under the UAE federal law.

ESTEEM BULLION FZCO shall maintain a register of all suspicious transactions that have been brought to the attention of its Compliance Officer or Compliance Unit, including transactions that are not reported to the AMLSCU.

The register shall contain details of the date on which the report is made, the person who made the report to its Compliance Officer and information sufficient to identify the relevant papers related to said reports.

Chapter 3 of the UAE Federal Law No. 4 of 2002 provides penalties for failure to report suspicious activities to the AMLSCU by those who are aware of a suspicious activity or transaction which may be a criminal offense, punishable by a fine or imprisonment or both.



18.1 Obligation to Report Suspicious Transaction

Whenever a reporting entity processes a transaction to which there is reasonable grounds to suspect that any property is the proceeds of crime, or is related to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or persons who finance terrorism, it should take reasonable measures to ascertain the purpose of that transaction and submit a report to the Centre, setting out the suspicion, within three (3) working days of forming that suspicion.

Further, a reporting entity is required to exercise caution when carrying out a transaction which it suspects to be related to money laundering or financing of terrorism. The Act also requires an STR to be submitted on attempted money laundering or financing of terrorism.

In exceptional cases (transactions that require immediate action), making a suspicious transaction report to the FIU does not prevent a reporting entity from reporting suspicions of money laundering or financing of terrorism directly to law enforcement agencies. Nevertheless, an STR still need to be submitted to the FIU. The FIU encourages reporting entities to maintain established relationships with law enforcement agencies.

18.2 Suspicious Transaction Reporting

- Suspicious Transactions Reports (STRs) play a pivotal role in the fight against money laundering and terrorist financing. information provided on STRs assist Law Enforcement Agencies in their investigations, resulting in the disruption of criminal and terrorist activities ultimately result in prosecution and imprisonment.
- Suspicious Transactions Reports (STRs) - within the meaning of the AML-CFT Law and its implementing AML-CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds which has reasonable grounds to suspect as constituting in whole or in part, and regardless of the amount or the timing—any of the following:
 - ✚ The proceeds of crime (whether designated as a misdemeanour or felony, and whether committed within the State or in another country in which it is also a crime);
 - ✚ Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations.
 - ✚ Being intended to be used in an activity related to such crimes.
- Wherein any employees who suspects or identifies red flags displayed by the customer, he shall ensure not to “tip-off” the customer and immediately escalate the same to the Compliance Officer.
- Compliance Officer shall review, scrutinize, and study records, the receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality.



- In case the Compliance Officer found reasonable grounds that such transactions be suspicious, ESTEEM BULLION FZCO shall adhere to the following:
 - ✚ Directly report STRs to the FIU's Go AML System without any delay.
 - ✚ Submit all supporting documents and appropriate justifications.
 - ✚ Respond to all documents or information requested by FIU.
 - ✚ All employees shall be available for interview and shall cooperate with the Law enforcement investigation.

18.3 Role of the Financial Intelligence Department

The FIU operates independently by legal and regulatory mandate as the central national agency with sole responsibility for performing the following functions:

- Receiving and analysing Suspicious Transactions Reports from FIs and DNFBPs, 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 its analysis, 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 other information to which it has access.

Under the aegis of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, and for the effective performance of its functions, the FIU maintains operational protocols with numerous national and international Competent Authorities. The Competent Authorities with which the FIU has informationsharing mechanisms in place include, among others, the following (in alphabetical order):

- ADGM (Abu Dhabi Global Market);
- Abu Dhabi Police General Headquarters;
- Dubai Financial Services Authority (DFSA);
- Dubai Gold and Commodities Exchange (DGCX);
- Dubai International Financial Centre;
- Dubai Multi Commodities Centre (DMCC);
- Dubai Police General Headquarters;
- Federal Customs Authority;
- Securities and Commodities Authority;
- Sharjah Police General Directorate.



Additionally, the FIU has been a member of the Egmont Group of Financial Intelligence Units since 2002 and maintains operational protocols for the international exchange of information with at least 45 other Financial Intelligence Units from around the world.

The types of information which the Financial Intelligence Department exchanges with other national and international Competent Authorities include, among others:

- Database search enquiries.
- Search and Freeze requests.
- Mutual Legal Assistance requests with international law enforcement/judicial authorities.

The Financial Intelligence Department thus links the public and private sectors in combating money laundering, the financing of terrorism and illegal organisations, as well as the proliferation of weapons of mass destruction. It also provides training, technical assistance and guidance on evolving standards and best practices to all stakeholders within the UAE for the strengthening of the country's AML/CFT framework.

19. Politically Exposed Persons (PEPs)

Due to their potential ability to influence government policies, determine the outcome of public funding or procurement decisions, or obtain access to public funds, politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective. The AML-CFT Law and the AML-CFT Decision define PEPs as:

- ❖ Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following:
 - ✚ Direct family members (of the PEP, who are spouses, children, spouses of children, parents)
 - ✚ Associates known to be close to the PEP, which include:
 - ✚ Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP.
 - ✚ Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

In addition to undertaking normal customer due diligence procedures, to put in place appropriate risk management systems to determine whether a customer, Beneficial Owner, beneficiary, or controlling person is a PEP. Also required to take reasonable measures to establish the source of funds of customers and Beneficial Owners identified as PEPs.



- + Implementing automated AML/CFT filtering systems which screen customer and transaction information for matches with known PEPs.
- + Incorporating thorough background searches into their CDD and EDD procedures, using tools such as:
 - + Manual internet search protocols.
 - + Public or private databases.
 - + Publicly accessible or subscription information aggregation services.
 - + Commercially available background investigation services

If a customer (or Beneficial Owner, beneficiary, or controlling person) is identified as a PEP. In this regard, they should also evaluate the legitimacy of the source of funds, including making reasonable investigations into the individual's professional and financial background prior to becoming a PEP, if necessary.

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

- + An existing customer (or Beneficial Owner, beneficiary, or controlling person) becomes, or is newly identified as, a PEP.
- + An existing PEP Business Relationship is reviewed, and the customer due diligence information is updated, either on a periodic or an interim basis, according to the organisation's internal policies and procedures.
- + A material transaction that appears unusual or out-of-pattern for the Business Relationship is identified in relation to a PEP.
- + The beneficiary or Beneficial Owner of a life insurance policy or family takaful insurance policy is identified as a PEP, in which case the overall Business Relationship should also be thoroughly examined, and consideration given to filing a STR.

With regard to identified Domestic PEPs and individuals who were previously (but are no longer) entrusted with prominent functions at international organisations, the AML-CFT Decision provides that our company implement the measures described above when, apart from their PEP status, the Business Relationships associated with such persons could be classified as high-risk for any other reason.



20. Transaction Monitoring

Monitoring refers to the monitoring of customer transactions, including assessing historical/current customer information and interactions to provide a complete picture of customer activity. ESTEEM BULLION FZCO monitors all the transactions for detecting any unusual/ suspicious activity based on ongoing transactions (both real time and post transaction) for all products and services using a Risk-Based Approach.

The Company pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The Company have understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity in order to effectively control and reduce the risk. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should be noted and must be reported to the Corporate Office.

As part of monitoring and control activities, the Company procures that the personnel carrying out these activities have access to internal information resources. Monitoring and control activities include but are not limited to the following:

- ❖ Monitoring and controlling customers and transactions in the high risk group,
- ❖ Monitoring and controlling transactions conducted with risky countries,
- ❖ Monitoring and controlling complex and extraordinary transactions,
- ❖ Controlling, through sampling method, whether the transactions exceeding a predetermined limit are consistent with the customer profile,
- ❖ Monitoring and controlling linked transactions which, when handled together, are exceeding the limit requiring customer identification,
- ❖ Controlling completing and updating the information and documents about the customer which have to be kept in electronic media or in writing and the compulsory information which have to be included in electronic transfer messages,
- ❖ Monitoring whether a transaction conducted by the customer is consistent with the information about the customer's business, risk profile and fund resources on a permanent basis throughout the term of the business relationship;
- ❖ Risk-based control of newly introduced products and services which may be exposed to abuse due to technological development.

20.1 Periodical Review

This Policy shall be reviewed on at least an annual basis. All reviews shall take into account legislative changes regarding AML and CFT and shall examine the previous 12 months implementation of the Policy, considering improvement opportunities.



20.2 Trustee, Nominee Or Fiduciary Accounts

- ESTEEM BULLION FZCO shall establish whether the applicant for business relationship is acting on behalf of another person as trustee, nominee or agent. AESTEEM BULLION FZCO should obtain satisfactory evidence of the identity of such agents and authorized signatories, and the nature of their trustee or nominee capacity and duties.
- Where ESTEEM BULLION FZCO entertains doubts as to whether the trustee, nominee or agent is being used as a dummy in circumvention of existing laws, it shall immediately make further inquiries to verify the status of the business relationship between the parties. If satisfactory evidence of the beneficial owners cannot be obtained, ESTEEM BULLION FZCO shall consider whether to proceed with the business, bearing in mind the “Know-Your-Customer” principle. If they decide to proceed, they are to record any misgiving and give extra attention to monitoring the account in question.

20.3 Transaction Undertaken On Behalf Of Account Holder or Non-Account Holders

- a. Where transactions are undertaken on behalf of account holders of ESTEEM BULLION FZCO, particular care shall be taken to ensure that the person giving instructions is authorized to do so by the account holder.
- b. Transactions undertaken for non-account holders demand special care and vigilance. Where the transaction involves significant amounts, the customer should be asked to produce positive evidence of identity including nationality, the purposes of the transaction and the sources of the funds.

21. Independent Review of Anti-Money Laundering Program

21.1 Introduction

Independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. It is deemed complete when it includes the requirement for an Independent, regular review to be performed to assess the adequacy of the policies and procedures, systems and controls and the Compliance Officer’s function.

21.2 Objectives

- To test the effectiveness and adequacy of the internal policies, controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organizations.
- To suggest changes and modifications in procedures to have more effective controls in the fight against money laundering and terrorism financing.



21.3 Guidelines

Both internal & external audits play an important role in evaluating the procedures of the Company. In order to ensure that its AML compliance program is effective and adequate in assisting it to meet its regulatory obligations, the Company must arrange for the following independent testing.

22. Red Flags

Red flag is a single factor that signals a transaction is unusual and possibly suspicious. Customer/ transactions like those mentioned below may warrant attention. Just because a customer appears on the list does not mean that he/she is involved in illegal activity. It only means that the transaction of customer requires closer scrutiny.

22.1 Red Flag Indicators for TF and PF

Accurately identifying and assessing the TF and PF risks of a customer or business relationship is critical for appropriately managing these risks.

A single indicator on its own may seem insignificant, but when combined with others it could provide reasonable grounds to suspect that the transaction is related to TF or PF activity.

i. Red Flag Indicators for TF

Potentially Suspicious Activity That May Indicate Terrorist Financing Published in the FFIEC BSA/AML Examination Manual.

A. Activity Inconsistent with the Customer's Business:

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.



B. Funds Transfers:

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher risk countries.

C. Other Transactions That Appear Unusual or Suspicious:

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

D. Terrorist Financing Indicators Published by FINTRAC (Canada's Financial Intelligence Unit)

- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner.
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.



- Transactions involve individual(s) or entity (ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates individual(s) or entity (ies) may be linked to a terrorist organization or terrorist activities.
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Individual or entity's online presence supports violent extremism or radicalization.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowd funding initiative, charity, non-profit organization, non-government organization, etc.).

ii. Red Flag Indicators for PF

Indicators of Possible Proliferation Financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing

- Transaction involves a person or entity in foreign country of proliferation concern.
- Transaction involves a person or entity in foreign country of diversion concern.
- The customer or counterparty or its address is similar to one of the parties found on publicly available lists of “denied persons” or has a history of export control contraventions.
- Customer activity does not match business profile, or end-user information does not match end user’s business profile.
- A freight forwarding firm is listed as the product’s final destination.
- Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- Transaction involves possible shell companies (e.g. companies do not have a high level of capitalization or display other shell company indicators).
- Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Trade finance transactions involve a shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import goods involved?)
- Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.



- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
- Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
- New customer requests letter of credit transaction awaiting approval of new account.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
- Involvement of items controlled under WMD export control regimes or national control regimes.
- Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
- Use of cash or precious metals (e.g. gold) in transactions for industrial items.
- Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
- Involvement of a customer or counterparty, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.
- Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions.
- Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
- Involvement of a university in a country of proliferation concern.
- Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
- Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.
- Use of personal account to purchase industrial items.

iii. Red Flag Indicators for Potential Sanctions Circumventions

Some Red Flags or Situations to Identify Potential Sanctions Circumventions Published in the Executive Office’s “Typologies on the Circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction”

The following are some red flags or situations that could be looked at more closely or monitored by financial institutions and designated non-financial businesses or professions to identify potential sanctions circumventions of your clients, their business, or their transactions.



- Dealings in sectors vulnerable for terrorist financing and/or proliferation of weapons of mass destructions, for example:
 - ✚ Financial sector
 - ✚ Hawalas or other money transfer services providers
 - ✚ Oil and gas sector
 - ✚ Non-profit organizations
 - ✚ International trade
- Dealings, directly or through a client of your client, with high-risk countries for terrorism financing.
- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.
- Dealings with sanctioned goods or under embargo. For example:
 - ✚ Weapons
 - ✚ Oil or other commodities
 - ✚ Luxury goods (for DPRK sanctions)
- Dealings with dual-used goods.
- Dealings with controlled substances.
- Identifying documents that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- Use of intermediaries.
- When the flows of funds exceed those of normal business (revenues or turnover).
- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
 - For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
 - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.
- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.
- Carrying out of multiple ATM cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or in the border of sanctioned countries
- Irregularities during the CDD process which could include, but is not limited to:
 - ✚ Inaccurate information about the source of funds and/or the relationship with the counterparty.
 - ✚ Refusal to honor requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.
 - ✚ Suspicion of forged identity documents.



23. Tipping off

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

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

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

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

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

24. Employee Behavior

Employees behavior is observed at all times and we take notice of the red flags like an employee living a life which is not supported by his salary, anyone who is not taking a vacation or if an employee is associated with unusually large numbers of transactions, etc.



25. Record Keeping

ESTEEM BULLION FZCO are obliged to maintain detailed records, documents, data and statistics for all financial transaction types, as well as a variety of record types and documents associated with their ML/FT risk assessment and mitigation measures, as specified in the relevant provisions of the AML-CFT Decision.

Required to maintain the records in an organised fashion so as to permit data analysis and the tracking of financial transactions, and to make the records available to the Competent Authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, depending on the circumstances, from the date of the most recent of any of the following events:

- Termination of the Business Relationship or the closing of a customer's account with the supervised institution.
- Completion of a casual transaction (in respect of a customer with whom no Business Relationship is established);
- Completion of an inspection of the records by the Supervisory Authorities.
- The issue date of a final judgment by the competent judicial authorities.
- Liquidation, dissolution, or other form of termination of a legal person or arrangement.

In order to fulfill their record-keeping obligations, and commensurate with the nature and size of their businesses, ESTEEM BULLION FZCO determine the appropriate policies, procedures and controls related to the adequate retention, organisation, and maintenance of records. The policies, procedures and controls is documented, approved by senior management, and communicated to appropriate levels of the organisation.

- Organisational roles and responsibilities in regard to the risk assessment, implementation, review and updating of policies, procedures and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures.
- Organisational roles and responsibilities in relation to record-keeping (including logging, cataloguing and organisation, archiving, handling and transferring of records and documents, as well as of the destruction of expired records)
- Physical and cyber security, and the protection of active and archived data and records from unauthorized access.
- Appropriate audit and quality assurance testing policies.



25.1 Required Record Types

The AML-CFT Law and AML-CFT Decision oblige ESTEEM BULLION FZCO to retain several types of records, which can be classified broadly into the following categories:

- **Financial Transaction Records:** This category relates to operational and statistical records, documents and information concerning all financial transactions executed or processed by the supervised institution, whether domestic or international in nature.

To retain the operational and statistical records, documents and information concerning all financial transactions executed or processed by the supervised institution, whether domestic or international in nature, and irrespective of the type of customer and whether or not a Business Relationship is maintained, for a minimum period of five (5) years. Some examples of the type of records, documents and information which must be retained include but are not limited to:

- Customer correspondence, requests or order forms related to the initiation and performance of all types of transactions;
- Customer payment advices, receipts, invoices, billing notifications, bills of exchange, statements of account, expense reimbursement requests or notifications;
- Credit-related correspondence and documentation, including those involving accounts receivable, cash advances or advance settlements, promissory notes, loans or guarantees and their amendments and supporting documents, disbursement or repayment records, collateral pledges, or any other form of customer credit;
- Deal tickets, trade blotters and ledgers, settlement and dividend payment records related to customer funds managed, legal structures or arrangements, or any other forms of asset trades or exchanges;
- Escrow or fiduciary account transaction records;
- Sale, purchase, lease, merger-acquisition, and similar agreements;
- Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates, and other information.

In addition to the above, ESTEEM BULLION FZCO will compile notes on any particularly large or unusual transactions and keep these notes as part of their records.

- **CDD Records:** This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:

- **Customer Information:** Retain all customer records and documents obtained through the performance of CDD measures in relation to Business Relationships, including customers, Beneficial Owners, beneficiaries, or other controlling persons. Examples of such records include but are not limited to:



- ✚ Customer account information and files;
- ✚ Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls);
- ✚ Copies of personal identification documents, KYC and CDD (including EDD and SDD) forms, profiles and supporting documentation, and results of due diligence background searches, queries and investigations.
- ✚ Customer risk assessment and classification records.

✚ **Company Information:** The AML-CFT Decision provides that the administrators, liquidators, or any other stakeholders involved in the dissolution of a company are obliged to retain the records, documents and information specified in the relevant articles for a minimum period of five (5) years from the date of its dissolution, liquidation or termination. These records pertain to corporate documents as well as to information on Beneficial Owners, legal shareholders, and senior managers. Such records include but are not limited to documents and information concerning:

- ✚ Company formation, registration, deregistration, liquidation, dissolution or expiry, including documents such as share registers, memoranda and articles of association, deeds of settlement and foundation charters, or similar documents, along with any amendments to them (whether the organisation is for-profit or not-for-profit);
- ✚ Changes to company information, such as name, registered address, legal representatives and corporate officers (directors, company secretary), or legal form;
- ✚ Identification and identity verification documents related to Beneficial Owners, shareholders, nominee shareholders, directors, senior management officers and, in the case of Legal Arrangements, settlors or founders, protectors, beneficiaries, trustees or executors, governing council or committee members, or similar controlling persons.

In order to fulfil their statutory record-keeping obligations in this regard, and commensurate with the nature and size of their businesses, engaged as corporate attorneys, trustees, or company service providers, administrators, liquidators, directors, or any other form of stakeholders) should determine the appropriate policies, procedures and controls related to the adequate retention, organisation, and maintenance of records.

✚ **Reliance on Third Parties to Undertake CDD:** ESTEEM BULLION FZCO are obliged to ensure that copies of all the necessary documents collected through the performance of CDD measures can be obtained upon request and without delay, and that the third parties adhere to the record-keeping provisions of the AML-CFT Decision.

In order to fulfil their statutory obligations, and commensurate with the nature and size of their businesses, ESTEEM BULLION FZCO determine the appropriate policies, procedures and controls related to the assessment, monitoring, and testing of third parties' record-retention frameworks.



- ✚ Organisational roles and responsibilities in regard to the assessment, monitoring and testing of the third party's policies, procedures and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures;
 - ✚ Organisational roles and responsibilities for the implementation of service-level agreements with third parties governing the provision of record-keeping services;
 - ✚ Operational procedures related to request and transfer of records and documents, as well as their physical and cyber security, and the protection of active and archived data and records from unauthorized access;
 - ✚ Appropriate audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework.
- ✚ **Ongoing Monitoring of Business Relationships:** to retain all customer records and documents obtained through the ongoing monitoring of Business Relationships. Examples of such records include but are not limited to:
- ✚ Transaction review, analysis, and investigation files, with their related correspondence;
 - ✚ Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls) related to transactions or their analysis and investigation;
 - ✚ Customer due diligence records, documents, profiles or information gathered in the course of reviewing, analysing or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions;
 - ✚ Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence
- ✚ **Suspicious Transaction Reports (STRs):** retain all records and documents pertaining to suspicious transaction reports and the results of all analysis or investigations performed. Such records relate to both internal STRs and those filed with the FIU, and include but are not limited to:
- ✚ Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence;
 - ✚ Competent authority request for information (RFIs), and their related investigation files and correspondence;
 - ✚ Customer due diligence and Business Relationship monitoring records, documents and information obtained in the course of analysing or investigating potentially suspicious transactions, and all internal or external correspondence or communication records associated with them;
 - ✚ STRs (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records, and all related correspondence;
 - ✚ Notes concerning feedback provided by the FIU with respect to reported Suspicious Transactions, as well as notes or records pertaining to any other actions taken by, or required by, the FIU.



26. Establishing an Effective Governance Framework

26.1 Adopt and Commit to a Policy for Managing Risks in Gold from CAHRAs

Regulated Entities must adopt a documented gold Supply Chain policy that incorporates the risks and risk mitigation measures. The policy and any supporting procedures should include details on the gold Supply Chain Due Diligence which the company will assess itself and the activities and relationships of suppliers. The policy should at least contain the following elements, which are consistent with OECD model Supply Chain policy as listed in Annex II of OECD Guidance.

- a) Scope
- b) Roles and responsibilities of employees, management and Board of Directors
- c) Know Your Counterparty (KYC) and Customer Due Diligence measures
- d) Supply Chain risk assessment and risk mitigation process
- e) Ongoing monitoring measures
- f) Independent audit mechanism
- g) Record retention requirements
- h) Training program

26.2 Establish Management Structures to Implement Supply Chain Due Diligence.

Regulated Entities must establish internal governance system to effectively implement and maintain a Supply Chain Due Diligence program on an ongoing basis. The minimum requirements are as follows:

The board of directors, or equivalent, should acquire the necessary knowledge and experience, or utilise external expert advisors, to:

- ✚ provide oversight of the Supply Chain Due Diligence framework and outcomes;
- ✚ ensure that effective structures and communication processes are in place for critical information sharing;
- ✚ assess the effectiveness of the Supply Chain Due Diligence policies and processes on an ongoing basis;
- ✚ ensure that the compliance officer's responsibilities include gold Supply Chain Due Diligence matters;
- ✚ ensure the availability of required resources to manage the Supply Chain Due Diligence process;
- ✚ delegate authority and assign responsibility to staff whom are equipped with the necessary competence, knowledge and experience to manage the Supply Chain Due Diligence process; and put in-place an organizational structure that can effectively communicate critical information, including the Supply Chain Due Diligence policies and procedures, to relevant employees.



27. Identification and Assessment of the Supply Chain Risk

27.1 Conduct Supply Chain Due Diligence to identify potential risks

Regulated Entities must identify and assess the risks in the Supply Chain to carry out required due diligence. Due diligence must be undertaken before entering a new business relationship with a supplier and should be carried out on an ongoing basis. Conducting risk assessment will help to tailor the due diligence according to the risks identified. Where high risk Supply Chain is identified, enhanced due diligence measures should be taken to mitigate the risks. Regulated Entities should use the management system put in place under Establishing an Effective Governance Framework of the Regulations to effectively identify and assess risks through their Supply Chain.

If a Regulated Entity can reasonably determine based on the information collected under Establishing an Effective Governance Framework of the Regulations that it does not deal in gold mined, transported or traded in a CAHRA, no additional due diligence is required. The management systems established under Establishing an Effective Governance Framework should be maintained and regularly reviewed. However, Regulated Entities should ensure that the applicable AML/CFT measures in line with AML/CFT Legislation and other Applicable Laws and Regulations are complied with which are applicable to Regulated Entities being DNFBPs.

The risk assessment should be carried out using risk factors broadly categorized in:

➤ Counterparty Risk Factors:

- ✚ KYC information of the Regulated Entity's suppliers as identified under Establishing an of the Regulations (including information about the origin and transportation of the gold).
- ✚ Identified Red Flags in the Supply Chain.
- ✚ Number of participants in the Supply Chain.
- ✚ Extent and effectiveness of due diligence practices of a counterparty.
- ✚ Counterparty's conformance with OECD Guidance while engaging in sourcing of gold.
- ✚ Whether a counterparty's due diligence practices have been audited by a qualified third-party auditor in line with applicable responsible sourcing mechanism.
- ✚ Length of establishment of supplier or other counterparties in the Supply Chain.
- ✚ Complexity in the ownership structure of the counterparties such as presence multiple layers of ownership and involvement of trust and similar vehicles apparently for purpose of anonymity.
- ✚ Size of mining operations of a supplier (ASM or LSM), if applicable
- ✚ Involvement of any PEPs that have been entrusted with prominent public functions or individuals who are closely related to such individuals.
- ✚ Adverse media/Sanctions listing findings through the screening of the suppliers and other actors in the supply chain.



➤ Geographical Risk Factors:

Regulated Entities should be able to identify the location and origin of the gold sourced by them using reasonable efforts. Different origins have different risks and require different treatments. Identification of gold origin should be evidence based and collected through suppliers and entity's own research.

- ✚ **Mined Gold:** The origin of mined gold is the mine itself except in cases of a mining by-product such as gold obtained through mining of copper. A refiner should be able to identify misrepresentation of mined gold as by-product through appropriate due diligence.
- ✚ **Recyclable Gold:** The origin of recycled gold is the point at which it becomes recyclable such as when it is first sold back to a gold recycler/Refiner. A refiner's due diligence should include measures to identify attempts to misrepresent the origin of newly mined gold through recycled gold.
- ✚ **Grandfathered Stocks:** If a verifiable date from prior to 1 January 2012, no determination of origin is required. However, if red flags are identified with regard to violation of AML regulations or international sanctions, further scrutiny of the Supply Chain is warranted.

Location-based risk identification should be carried out using reasonable efforts and recognized sources of information. At a minimum, the following risk factors should be utilized for risk identification.

- ✚ The AML/CFT and other regulatory environments in the supplier's jurisdiction or location which is part of Supply Chain.
- ✚ Level of conflicts or human rights abuses in any location comprising part of the Supply Chain through reliable resources.
- ✚ Level of involvement of widespread bribery and corruption through reliable resources.
- ✚ The level of involvement or potential involvement of any criminal organization.
- ✚ The level of access from a location comprising part of the Supply Chain to nearby markets or processing operations that are termed as CAHRA.
- ✚ The level of enforcement of laws addressing significant criminal activity.
- ✚ Payment mechanism used (e.g. formal banking system vs. non-banking system).
- ✚ The existence of international sanctions and/or embargoes that have been directed against the country and/or individuals/entities in that country by the UN Security Council and/or UAE from time to time.
- ✚ Involvement of countries identified as CAHRA.

➤ Transactions Risk Factors:

- ✚ Inconsistency of transaction with the local or market practices (amount, quality, potential profit, etc.).
- ✚ Inconsistency of volumes, types and concentrations of material compared with previous shipments with the same client.
- ✚ Use of excessive cash in transactions.
- ✚ Attempted structuring of transactions to make payments to avoid government thresholds.



- ✚ Identified risks and severability and probability of adverse impacts of the applicable transaction.
- ✚ Gold that are transported which are not reasonably reconciled with the declared location of the origin
- ✚ Unexplained geographic distance in the Supply Chain.

➤ **Product Risk Factors:**

- ✚ The nature of the gold supplied such as, ASM or LSM gold, gold by-product, melted recyclable gold and unprocessed recyclable gold. The risk may vary from product to product.
- ✚ Level of concentration of gold in the supplied gold

28. Management of the Supply Chain Risk

Regulated Entities should evaluate and respond to identified risks through EDD in order to mitigate the identified risks. The following steps are minimum expected in order to mitigate the risks identified. Regulated Entities are encouraged to take into account the potential social and economic impacts of risk mitigation measures adopted by them.

A risk management plan should be subject to continuous review based on changes in circumstances related to business, operations or supply base, risk nature, or a major change in applicable rules and regulations.

29. What are Targeted Financial Sanctions (TFS)?

- Asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
- Designated persons and entities – Lists of “bad actors” who threaten the world peace (terrorism / proliferation)
- The lists are updated by the Security Council regularly
- UN member countries can't do financial dealings with such designated individuals and entities.



29.1 What is United Nations Security Council Resolution (UNSCR)?

- UN Security Council – Global Policeman
- Issue binding obligatory orders to members
- Famous for imposing sanction measures on countries (and individuals)
- Financial sanction measures are relevant to Financial Institutions



29.2 The FATF's Commitment to TFS

- FATF Recommendation 6 (Targeted Financial Sanctions related to Terrorism and Terrorist Financing) and 7 (Targeted Financial Sanctions related to Proliferation) required to implement the targeted financial sanctions regimes to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing and proliferation/WMD and its financing.
- Features of FATF Recommendation 6 – TFS related to Terrorism and Terrorist Financing (Source: FATF Methodology 2013)
 - ✚ Countries are to identify and designate a competent authority for proposing persons/entities
 - ✚ Have mechanisms for identifying targets for designation
 - ✚ Standard of proof: “reasonable grounds” or “reasonable basis”
 - ✚ Implement TFS without delay
 - ✚ Identify DOMESTIC competent authorities to implement and enforce TFS.

29.3 What is Proliferation Financing of Weapons of Mass Destruction (PF-WMD)?

- ✚ Providing funds for the rapid construction of WMD (Chemical/Biological/Radio Active/Nuclear – CBRN)
- ✚ State actors (governments) and non-state actors (individuals and organizations)
- ✚ Closely associated with science and technological research projects
- ✚ Separate UNSCRs for state and non-state actors
- ✚ Currently, North Korea (DPRK) and Iran have been designated as state actors



29.4 UN Security Council's Approach to Counter TF and PF-WMD

- ✚ UNSCR 1373 (2001)* – for local terrorists, UNSCR 1267 (1999)* – for Al-Qaida and ISIL, and UNSCR 1988 (2011)* for Taliban (CTF)
- ✚ Global approach under UNSCR 1540 (2004) and its successor resolutions (Non-state actors) (CPF-WMD)
- ✚ Country-specific approach under UNSCR 1718 (2006) and UNSCR 2231 (2015) and their successor resolutions (State actors) (CPF-WMD).



29.5 UNSCRs which are Relevant to You as FIs

- + Relevant because they are associated with TFS regimes
 - UNSCR 1267 and related resolutions
- + Al-Qaida and ISIL related individuals and entities
 - UNSCR 1988 and related resolutions
- + Taliban related individuals and entities
 - UNSCR 1373 and related resolutions
- + Local terrorist related individuals and entities (LTTE)
 - UNSCR 1718 and related resolutions
- + North Korea related individuals and entities – State Actors
 - UNSCR 2231 and related resolutions
- + Iran related individuals and entities – State Actors
 - UNSCR 1540 and related resolutions
- + Individuals and organizations (no list!) – Non-state Actors

29.6 Legislation On Financial

The DNFBPs shall without delay.

- + Freeze all the funds held by it in the name of a designated entity;
- + Inform the Attorney-General and the Financial Intelligence Unit that a designated entity has funds with the DNFBPs providing all details of such funds; and
- + Inform the designated entity that the funds held at the DNFBPs have been frozen.

29.7 The Obligation to Freeze ‘Without Delay’ defined

The Glossary of the FATF Recommendations defines ‘without delay’, with respect to the Al-Qaida/Taliban sanctions regimes, as ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, or the 1988 Committee). For the purposes of resolution 1373(2001), the term without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organization. In both cases, the term without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organizations, and those who finance terrorism.

29.8 Protection against Liability for Reporting Persons

The TFS Law and the AML-CFT Decision provide Designated Non-Financial Businesses and Professions, as well as their board members, employees and authorized representatives, with protection from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the Competent Authority.



TFS are implemented in the UAE pursuant to UNSCRs in relation to:

a. Terrorism and terrorist financing:

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

b. The proliferation of weapons of mass destruction (WMD):

1. Democratic People's Republic of Korea (DPRK): nuclear-related, other weapons of mass destruction-related and ballistic missile-related programmes.	UNSCR 1718 (2006) and its successor resolutions
2. Islamic Republic of Iran: nuclear programme	UNSCR 2231 (2015)

c. Other UN sanctions regimes with TFS:

1. Somalia	UNSCR 1844 (2008)
2. Iraq	UNSCR 1483 (2003)
3. Democratic Republic of Congo (DRC)	UNSCR 1596 (2005) & UNSCR 1807
4. Related to the involvement of terrorist bombing in Beirut (2005) plus restrictive measures in relation to UNSCR 1701 (2006) on Lebanon	UNSCR 1636 (2005) & UNSCR 1701 (2006)
5. Libya	UNSCR 1970 (2011)
6. Central African Republic (CAR)	UNSCR 2127 (2013)
7. South Sudan	UNSCR 2140 (2014)
8. Mali	UNSCR 2206 (2015)
9. Yemen	UNSCR 2374 (2017)



29.9 Describe your jurisdiction's sanctions regime.

The United Arab Emirates (“UAE”) has a complex sanctions regime based on a variety of sources. Sanctions are based on diverse interests, including political, economic, and national security interests. Due to the rapidly changing nature of such interests, sanctions are susceptible to significant and constant changes.

Sanctions in the UAE are usually imposed at a federal level, through a variety of methods, including, by way of example:

- ✚ Adding sanctioned persons to local lists and the United Nations (“UN”) sanctions list: This is effected by issuing local terrorism lists (“Local Lists”) and implementing the sanctions passed by the UN Sanctions Committee (“Sanctions List”) pursuant to Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and illegal Organizations (“AMLCFT Law”), Cabinet Decision No.10 2019 concerning the Implementing Regulation of the AMLCFT Law (“New Sanctions Regulations”) the recent Cabinet Decision No 74 of 2020 concerning the UAE List of Terrorists and the Implementation of UN Security Council Decisions Relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of Mass Destruction, and the Relevant Resolutions (“New Sanctions Regulations”) and Federal Law No. 7 of 2014 on Combatting Terrorism Offences. Guidance was issued on targeted financial sanctions by the Executive Office of the Committee for Goods and Materials subject to Import and Export Control (“Office”) on 6 May 2021 further setting out the implementation of the New Sanctions Regulations (the “New SR Guidance”).

UAE and international sanctions such as those of the UN, Office of Foreign Assets Control (“OFAC”) and the European Union (“EU”), as applicable. As a member of the UN, the UAE is required to comply with all sanctions passed by the UN Security Council.

29.10 There have been significant changes or developments impacting the UAE sanctions regime over the past 12 months.

Notably, from a legislative framework perspective, the UAE’s previous sanctions regulations and implementation regulations were abrogated, and new such legislation was issued. From a substantial perspective, among other changes, compliance obligations and required steps by UAE persons have increased, as illustrated in the New SR Guidance.

A. Legal Basis/Sanctions Authorities

The legal or administrative authorities for imposing sanctions.

The Supreme Council for National Security, the UAE Cabinet and the UN Security Council are the ultimate entities responsible for imposing sanctions. The Supreme Council for National Security proposes sanctions both internally and to the UN Sanctions Committee pursuant to Article 2 of the New Sanctions Regulations.



B. Jurisdiction implements United Nations sanctions.

The process of significant ways in which company implemented United Nations sanctions.

DNFBPs and FIs are subject to additional obligations as set out in the New SR Guidance. These include setting internal controls and procedures to ensure compliance with the New Sanctions Regulations, as well as policies and procedures to prohibit staff from informing any customer or third party of impending freezing action.

It is worth noting that in certain cases, sanctions imposed by the UN may have already been implemented by the UAE on other grounds and included in Local Lists, e.g., as a result of its membership in the Terrorist Financing Targeting Centre (“TFTC”).

The UAE is a member of three main regional bodies that issue sanctions – the Arab League, the TFTC and the Gulf Cooperation Council (“GCC”).

- ✚ **Arab League:** The UAE implements sanctions adopted by the Arab League on an ad hoc basis.
- ✚ **TFTC:** Members of the TFTC consist of the United States and certain GCC countries.
- ✚ The UAE implements all sanctions designated by the TFTC by issuing the Local Lists referred to above. TFTC designated sanctions are also available on the US’s treasury government website.
- ✚ **GCC:** The UAE is a member of the GCC, which consists of six member states. The Charter of the GCC sets up a framework that would permit the joint establishment of foreign policies and therefore issuance of sanctions. Although the GCC has, in the past, made announcements with respect to its members’ stance on foreign policy. It has not, at the date hereof, issued any sanctions as such.

C. Jurisdictions maintain any lists of sanctioned individuals and entities.

Were the individuals and entities: a) added to those sanctions lists and b) removed from those sanctions lists.

The UAE maintains two lists of sanctions individuals and entities:

- ✚ **Local Lists:** These lists consist of local terrorism lists issued pursuant to Federal Law No. 7 of 2014 on combatting terrorism offences (“Anti-Terrorism Law”) and the New Sanctions Regulations. Decisions of listing, removal and re-listing on Local Lists enter into effect when issued by the UAE Cabinet and when published in the Official Gazette. Such decisions are also published in audio-visual and print media of the UAE, in both Arabic and English.
- ✚ **Sanctions List:** This list consists of the sanctions list issued by the UN Security Council. Additions and/or removal from the sanctions list are effected by the UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.

D. Can the public access those lists?

Both the consolidated Local List and Sanctions List are available via the following links:

- a. With respect to the Local List (<https://www.uaecic.gov.ae/en-us/un-page>)
- b. With respect to the Sanctions List (<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>)

There is also a direct link to the UN sanctions on the official website.



E. Comprehensive sanctions or embargoes against countries or regions

The UAE used to maintain comprehensive sanctions or embargoes on Qatar and Israel, however, these were recently removed and there are no current comprehensive sanctions or embargoes on countries as such. By implementing the UN's sanctions, the UAE does have targeted sanctions against Central African Republic, Congo, Iraq, Libya, Mali, Somalia, South Sudan and Yemen.

F. Jurisdiction maintains any other sanctions.

In addition, to the above-mentioned sanctions, the UAE, the regulated FIs in the UAE, also takes into consideration sanctions imposed by the EU and OFAC; however, where implemented, such sanctions would be added to its lists accordingly.

G. Implantation of Sanctions Laws and Regulations

Parties and transactions are subject to your jurisdiction's sanctions laws and regulations. For example, do sanctions restrictions apply based on the nationality of the parties involved or the location where the transactions take place?

The parties and transactions subject to UAE's sanctions laws and regulations depend on the nature of and reasons for the sanctions.

Certain sanctions are more narrowly targeted than others. With respect to sanctions targeted at specific individuals and organizations (e.g. under Local Lists), restrictions would not apply based on nationality but rather on identity or affiliations. With respect to more comprehensive sanctions targeted at governments, such sanctions can apply based in the nationality of persons involved.

Sanctions can also apply on the location where the transaction takes places, this is particularly relevant where sanctions are targeting trade with a certain country or the country imposing the sanction refuses to recognize or accept deals involving the currency of a certain country, as is the case with Iran.

H. Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Under Article 15 of the New Sanctions Regulations and under the New SR Guidance, there is an express obligation on FIs, DNFBPs, and all natural and legal persons to block or freeze funds or other property belonging to persons on the sanctions list ("Designated Persons").

1. If a match is identified with a Designated Person, they must freeze all funds owned by such person, prohibit the making of funds available, and notify the Office of such measures within two business days of taking such measures.
2. In addition to the above, FIs and DNFBPs must set and implement internal controls and procedures as well as policies and procedures to ensure their and their staff's compliance with the New Sanctions Regulations and that no one tips off any Designated Person of impending measures.

I. Are there licenses available that would authorize activities otherwise prohibited by sanctions?

There are no licenses available that would authorize activities otherwise prohibited by sanctions per se. However, special licenses may be required to conduct activities more susceptible to the possible breach of sanctions; for example, pursuant to the Commodities Law, strategic goods and dual –use items, such as arms and military hardware, chemical and biological materials cannot be exported or re-exported without a special license.



J. Are there any sanctions related reporting requirements? When must reports be filed and what information must be reported?

Multiple laws and regulations, including Article 15 of the AMLCFT Law, impose an obligation on FIs and DFNBPs to report to the relevant financial regulator any suspicion or any situation in which they have reasonable grounds to suspect a transaction or funds is related to a money laundering crime, related predicate offences, financing of terrorism or illegal organizations.

K. The government conveys its compliance expectations.

Are certain entities required to maintain compliance programs? What are the elements of a compliance program required (or recommended) by the competent regulator(s)?

The government conveys its compliance expectations by circulating circulars and directives as well as issuing laws, regulations and guidance, in particular its New SR Guidance.

Article 16 of the AMLCFT Law, as well as the New SR Guidance, require FIs and DFNBPs to develop internal policies, controls, and procedures to enable them to manage the risks identified and mitigate them.

30 Money Laundering Penalties under UAE Federal Law no (20) of 2018

Articles 14 to 31 of the law describe penalties concerning money laundering offenses, as follows:

Article 14:

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

- A. Warning
- B. Administrative penalties of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) for each violation.
- C. Banning the violator from working in the sector related to the violation for the period determined by the supervisory authority.
- D. Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.
- E. Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.



- F. Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority.
- G. Cancel the License.

Article 15:

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

Article 22:

1. Any person who commits or attempts to commit any of the acts set forth in Clause (1) of Article 2 of this Decree-Law shall be sentenced to imprisonment for a period not exceeding ten years and to a fine of no less than (100,000) AED one hundred thousand and not exceeding (5,000,000) AED five Million or either one of these two penalties.

A temporary imprisonment and a fine of no less than AED 300,000 (three hundred thousand dirham) and no more than AED 10,000,000 (ten million dirham) shall be applied if the perpetrator of a money laundering crime commits any of the following acts:

- A. If he abuses his influence or the power granted to him by his profession or professional activities.
 - B. If the crime is committed through a non-profit organization.
 - C. If the crime is committed through an organized crime group.
 - D. In case of Recidivism
2. An attempt to commit a money laundering offense shall be punishable by the full penalty prescribed for it.
 3. A life imprisonment sanction or temporary imprisonment of no less than (10) ten years and penalty of no less than AED 300,000 (three hundred thousand dirham) and no more than AED 10,000,000 (ten million dirham) is applied to anyone who uses Proceeds for terrorist financing.
 4. A temporary imprisonment sanction and a penalty of no less than AED 300,000 (three hundred thousand dirham) shall be applicable to anyone who uses the Proceeds in financing illegal organizations.



5. The Court may commute or exempt from the sentence imposed on the offenders if they provide the judicial or administrative authorities with information relating to any of the offenses punishable in this article, when this leads to the disclosure, prosecution, or arrest of the perpetrators.

Article 23:

1. A penalty of no less than AED 500,000 (five hundred thousand) and no more than AED 50,000,000 (fifty million dirham) shall apply to any legal person whose representatives or managers, or agents commit for its account or its name any of the crimes mentioned in this Decree-Law.
2. If the legal person is convicted with terrorism financing crime, the court will order its dissolution and closure of its offices where its activity is performed.
3. Upon issuance of the indictment, the court shall order the publishing of a summary of the judgment by the appropriate means at the expense of the condemned party.

Article 24:

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

Article 25:

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

Article 28:

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



Article 30:

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

Article 31:

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

