# ANTIMONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANIZATIONS

## (POLICIES & PROCEDURE MANUAL)

**VERSION 5.1**
**17 Nov 2025**
**Version control**

| | |
|---|---|
| V1 | Parent document |
| V2 | ***Sections 4.1.2, 4.2.2 & 4.5.2:***<br>*ID verification for non-resident individuals, non-resident legal entities and EDD measures* |
| V3 | ***Sections 4.7 & 4.8:***<br>*Transaction Monitoring (TM) and Trigger Event Reviews (TE) were updated.*<br><br>***Section 4.9:***<br>*Added a separate section for Periodic Reviews*<br><br>*Name of **Client Risk Profiling (CRP)** template changed to **CRA (Client Risk Assessment)** template* |
| V4 | ***Section 3.1 (Business Risk Assessment)***<br>*Expanded the RBA*<br><br>***Section 4 (Client Due Diligence)***<br>*More clarification of covered transactions and core components of counterparty identification*<br><br>***4.2.1. ID verification of locally registered entities***<br>*eDocument verification number for local non-individual clients*<br><br>***4.4.3, 4.4.4 & 4.4.5 –** expanded these sections to give more clarity on documenting the analysis of Adverse Media and PEP*<br><br>***Section 5.1.2 CO responsibilities***<br>*Reference to appendix 13 (semi-annual AML report submission)*<br><br>***Section 5.5 Cash Acceptance Procedure***<br>*Added approval matrix for cash acceptance*<br><br>***Appendix 1:***<br>*CRA template – included section for name of client and date. Finer modification to scoring guidelines*<br><br>***Appendix 2:***<br>*Refreshed the KYC form to be filled by clients to enable risk assessment*<br><br>***Appendix 13:***<br>*Included a format of a semi-annual AML report*<br><br>***Appendix 13, 14, 15:***<br>*Added templates for Semi-annual AML report, CO Job description, Risk Assessment Matrix* |
| V5 | ***Section 2 (Scope):***<br>*Included reference to CRA and CDD implementation guideline released by Ministry of Economy* |

[redacted]

**Owner / Manager**

**KHRYSOS TRADING FZCO**

[redacted]

Confidential - KHRYSOS TRADING DMCC

# Table of Contents



Confidential - KHRYSOS TRADING DMCC

# 1. INTRODUCTION

**KHRYSOS TRADING FZCO** (the 'DPMS entity) has prepared this manual to comply with UAE's Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (AML/CFT&IO).* In preparing this manual, the AML-CFT Law along with guidelines for designated non-financial businesses and professionals (DNFBP) have been studied together with the supplemental guideline for the Real Estate Sector.

**Definitions of Money-laundering:**

Money laundering is the process by which people attempt to conceal the origin of ownership of the proceeds of their illegal activities. The AML-CFT Law defines money laundering as engaging in any of the following acts willfully, having knowledge that the funds are the proceeds of a felony or a misdemeanor (i.e., a predicate offence):

- Facilitating the transfer or movement of proceeds or conducting any transaction which results in concealing or disguising their Illegal source.
- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.
- Acquiring, possessing or using proceeds upon receipt.
- Assisting the perpetrator of the predicate offense to escape punishment.

Both the AML-CFT Law and the AML-CFT Decision define "funds" in a very broad sense as "assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets." They likewise define "proceeds" as "funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds."

Therefore, to be considered money laundering, it is not necessary for any of the above-stipulated acts to involve only money or monetary instruments per se, but any number of tangible or intangible assets such as, but not limited to:

- Funds in bank or other financial accounts, including so-called virtual or crypto currencies.
- Financial instruments or securities, such as shares, bonds, notes, commercial paper, promissory notes, IOUs, share warrants, options, rights (including land rights), or other transferable securities or bearer negotiable instruments.
- Contracts, loan instruments, titles, claims, insurance policies, or their assignment.
- Intellectual property (including but not limited to patents or registered trademarks), royalties, licenses, or the rights thereto.
- Physical property, including but not limited to commodities, land, precious metals and stones, motor vehicles or vessels, works of art, or any other goods exchanged as payment-in-kind.

The **Financial Action Task Force on Money Laundering (FATF)**, which is recognized as the international standard setter for Anti-Money Laundering (AML) efforts, defines the term "money laundering" succinctly as "the processing of criminal proceeds to disguise their illegal origin" in order to" legitimize" the ill-gotten gains of crime. There are three stages to the money laundering process:

i. ***Placement*** (placing the proceeds of crime into the economy). This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into bank accounts, or by purchasing a series of financial instruments (such as cheques, money orders, etc.) that are then collected and deposited into accounts at other location. Placement vehicles could appear to be innocuous.

ii. ***Layering*** (to disguise the trail behind layers of transactions). The funds might be channelled through the purchase and sale of investment instruments, or the launderer may simply wire

the funds through a series of banks across the globe. In some instances, the launderer may attempt to disguise the transfers as payments for goods/services or a transfer from a reputable entity.

iii. ***Integration*** (integrating the proceeds of crime into the legitimate economy). This may include investing in real estate, luxury assets or business ventures.

The review system for the AML policies, procedures, systems and controls are robust and the entity ensures that these are reviewed at least annually which reflects good ethical practices.

The AML Policy should be structured in a way that the objectives and line of action are clearly defined.

The DPMS entity's Client Due Diligence (CDD) process flow has been depicted in figure 1 below.

Confidential - KHRYSOS TRADING DMCC

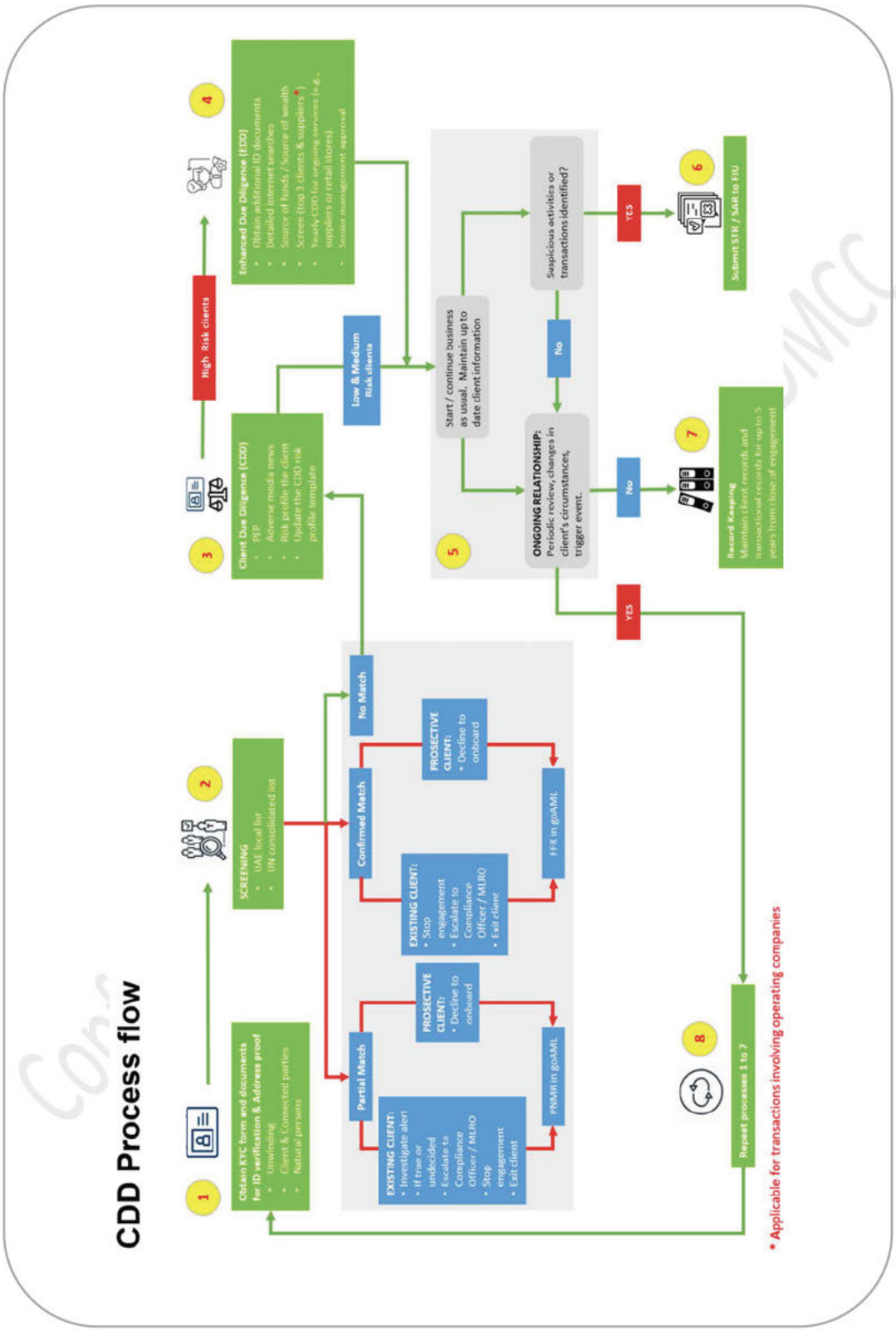


**Fig 1: Client Due Diligence process flow**

# 2. SCOPE

The standards set out in this procedure manual are minimum requirements based on the following AML-CFT legislations within UAE.

- Federal Decree law no. 20 of 2018 'AML law and amendments'
- Cabinet resolution no. 10 of 2019 'Implementation of the AML law'
- Cabinet decision no. 58 or 2020 'Regulating the Beneficiary Owner procedures.
- Cabinet resolution no. 74 of 2020 'Regarding terrorism list regulation'
- Cabinet decision no. 16 of 2021'Regarding the unified list of violations and administrative fines'
- Cabinet resolution no. 53 of 2021 'Concerning the administrative penalties against violators.

The entity reviews all regulatory notifications, thematic reviews and National Risk Assessment (NRA) reports as and when released and update this procedure manual wherever necessary.

This procedure manual is intended to assist the entity and its employees in complying with their obligations, arising from UAE legislation in relation to the prevention, recognition and reporting of money laundering.

This manual has been prepared in line with the following guidelines issued by the regulator,

- Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions
- Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions (Supplemental Guidance for Dealers in Precious Metals and Stones)
- Guidance on Targeted Financial Sanctions for FIs, DNFBPs and VASPs issued by Executive office of control & Non-proliferation (EOCN), UAE
- Guidance on Counter Proliferation Financing for Fis, DNFBPs and VASPs
- Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction
- Terrorist and Proliferation Financing Red Flags Guidance
- The following regulatory review reports of 2023
    - Thematic Review - Suspicious Activity and Transaction Reporting
    - Thematic Review - Targeted Financial Sanctions
- Implementation Guide for DNFBPs on Customer Risk-Assessment (CRA), Version 0.3.1.1 dated November 2024
- Implementation Guide for DNFBPs on Customer Due Diligence (CDD), Version 0.3.2.1 date December 2024
- Supplemental Guidance for Dealers in Precious Metals and Stones. (May 23, 2019)

Confidential - NIKKA TRADING DMCC

# 3. RISK BASED APPROACH (RBA)

3.1. The DPMS entity's approach to money laundering compliance is in line with the Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
FATF recommends that DNFBPs to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks. As per its Recommendation 1, a risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. Further, proliferation financing risk refers to the potential breach of the targeted financial sanctions obligations referred to in Recommendation 7 of FATF. The MoE has issued guidelines supporting these recommendations.

Fundamental to the RBA is a business risk assessment (BRA). The AML/ CFT Cabinet Decision obliges DNFBPs to document their risk assessment operation to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

3.2. The DPMS entity undertakes a Risk Based Approach (RBA) based on its exposure to risks associated with,

3.2.1. AML / CFT
3.2.2. Targeted Financial Sanctions (TFS)
3.2.3. Proliferation Financing (PF)

3.3. The Enterprise-wide risk associated with the above risks were assessed based on the following four risk factors. They are,

3.3.1. Customer / Client risk
3.3.2. Location / Geographical risk
3.3.3. Product & Services risk
3.3.4. Channel risk

3.4. The RBA considered the ***inherent risk*** against the above-mentioned risk factors which forms the basis for the controls designed and documented in the entity's policies and procedures manual. The entity periodically assesses the ***control operating effectiveness*** to arrive at the ***residual risk***. Where the residual risk is above the risk appetite of the entity, additional controls would be designed and published through a revision to this policies and procedure manual.

3.5. Further, prior to establishing a client relationship, the DPMS entity evaluates every client using the above-mentioned risk factors. Depending on the outcome of the entity's money laundering risk assessment of its client, the depth and intensity of CDD measures vary, which are documented in this manual.

3.6. The DPMS entity's risk appetite is MEDIUM (refer to APPENDIX 15: Risk Assessment Matrix).

3.7. The risk factors are scored based on a Client Risk Profiling template (Appendix -1) and clients are risk classified as under.

| | |
|---|---|
| – Low risk | CDD categorization = SDD (Simplified Due Diligence) |
| – Medium risk | CDD categorization = SDD (Standard Due Diligence) |
| – High risk | CDD categorization = EDD (Enhanced Due Diligence) |

3.8. The entity evaluates the client / counterparty based on the following risk factors:

- Client / Customer risk

Confidential - KHYSOS TRADING DMCC

- Product & services risk / Transaction risk
- Channel risk
- Location / Geographical risk

Based on the above risk factors, client due diligence (CDD) is performed for covered transactions.

# 4. CLIENT DUE DILIGENCE (CDD)

The trade in PMS consists of a complex ecosystem or supply chain and DPMS may perform a wide variety of roles or functions relating to the trade in PMS.

The DPMS entity participates only in one stage of the supply chain, which is Wholesale trade (Non-Manufactured Precious Metal Trading and Metal Ores Trading)

As per the AML-CFT Law and the AML-CFT decision, DPMS are obliged to apply AML/CFT measures whenever they carry out a single transaction, or series of transactions that appear to be related, whose monetary value equals or exceeds AED 55,000. This may include one or more transactions involving the same business relationship or customer, whether related to a single item or set of items; or it may also include one or more transactions which, in the judgment of the dealer, appear to be structured to avoid the established threshold. This is referred to as 'Covered Transactions'. In the below table a list of covered transactions is presented.

**List of covered transactions:**

In the following section, the list of covered transactions and which of those are applicable to the entity are covered in detail. For the sake of clarity, the threshold value adopted by the entity is AED 55,000.

| # | Type of transactions | Entity's response to transaction |
|---|---|---|
| 1 | ***Multiple invoices below threshold:*** Cash purchase of multiple PMS items exceeding AED 55,000 (threshold) with a request for multiple invoices. | In case of wholesale or retail, if multiple invoices are requested, with cash component against each invoice being below the threshold, but cumulative cash component is above the threshold then the entity applies the entire AML/CFT measures as stipulated by the regulator. Further, DPMSR is raised in goAML platform if the settlement value is in cash.<br><br>The DPMS entity settles its transactions in cash with its suppliers as it receives cash from its customers. |
| 2 | ***Multiple partial settlements:*** Aggregate of all partial cash settlements exceeding the threshold. Individual transaction may be below the threshold, however, on an aggregate basis, the cash is above the threshold. | In case of wholesale or retail, if cash component of partial settlements exceeds the threshold, then the entity applies the entire AML/CFT measures as stipulated by the regulator. Further, DPMSR is raised in goAML platform. |
| 3 | ***Transactions by seemingly different customers:*** Transactions performed by ostensibly different customers where each transaction is below the threshold, but total amount exceeds the threshold. | In case of wholesale or retail, if the entity notices behaviour of customers purporting to act as different individuals to remain under the AED 55,000 transaction threshold, then the entire AML/CFT measures as stipulated by the regulator is applied. Further, DPMSR is raised in goAML platform. |
| 4 | ***Settlement through cash and cash equivalents:*** Transaction in single or multiple PMS items settled partly through cash and partly through negotiable bearer instruments like money orders, | In case of wholesale or retail, if the DPMS entity notices that a customer settles his / her purchase partially with cash and the rest with the old ornaments, then the entire AML/CFT measures as stipulated by the regulator is applied. Further, DPMSR is raised in goAML platform. |

Confidential - KHRYSS TRADING LLC

| # | Type of transactions | Entity's response to transaction |
|---|---|---|
| | treasury bills, bearer bonds, promissory notes, etc. Together, the cash and cash equivalent exceed the threshold | |
| 5 | ***Settlement through trade-ins:*** Transaction in single or multiple PMS items settled partly through cash and the other part through a trade-in in a PMS items. Together, the cash and trade-in items exceed the threshold | In case of trade-in transactions, the entity applies the entire AML/CFT measures as stipulated by the regulator, should the trade-in value considered on its own or taken along with the cash component exceed the threshold. |
| 6 | ***Book value Vs market value of the PMS below threshold:*** Cash or cash equivalent used to settle a transaction in PMS exceeds the threshold, however, the book value or the market value is below the threshold | Since the entity is trading with pure gold, irrespective of the book value or market value, should the cash / cash equivalent in a transaction either singly or in aggregation exceed the threshold, then the entire AML/CFT measures as stipulated by the regulator is applied. Further, DPMSR is raised in goAML platform. |
| 7 | ***Sudden increase in volume of cash transactions:*** Sudden increase in the cash transactions for purchasing PMS of smaller values (like loose diamonds each valuing a fraction of the threshold limit). | The entity monitors its retail or wholesale transactions for such periodic vagaries in cash settlements as part of its ongoing monitoring. |
| 8 | ***Intrinsic value of trade-in PMS above threshold:*** Buy back value of PMS goods below the threshold and settled in cash, however, the intrinsic value is above the threshold | Buy back is treated like trade-in. The entity does not encourage such a transaction. However, should the intrinsic value of the traded-in PMS item be above the threshold, then the entity applies the entire AML/CFT measures as stipulated by the regulator. The entity applies the measures for its wholesale activities. |

Should any of the above-mentioned covered transactions occur, the entity applies the entire AML/CFT measures as stipulated by the AML/CFT guideline. For covered transactions, the entity applies both,

i. AML/CFT policies and procedures
ii. TFS policies and procedures

In case of non-covered transactions, decision issued by the UN Security Council under Chapter VII of the UN Charter is applied. These are stipulated by the "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations" - Guidelines for Designated Non-Financial Businesses and Professions (DNFBPs). More specifically section 10 of the guideline related to International Financial Sanctions.

The entity's procedures towards non-covered transactions are discussed in the 'TFS policies and procedures manual'.

i) The first step in the CDD process is to identify and verify the counterparty through their personal data and address. Know your customer (KYC) form given in appendix – 2 is used for collecting all appropriate documents from the counterparties. The form is duly signed by the authorized signatory (as per MoA) of the counterparty (legal entity) or in case of individual clients, the person(s) availing the services of the entity.

ii) The core components of counterparty identification are the following.

- Personal data, including details such as the name, passport or identity card number, country of issuance, date issuance and expiry date of the identity card or passport, nationality, date and place of birth (or date and place of establishment or incorporation, in the case of a legal person or arrangement); and

Confidential KHRYSO TRADING DMCC

- Principal address, including evidence of the permanent residential address of a natural person, or the registered address of a legal person or arrangement and tracing them through any intermediate entities.

iii) In case of corporate counterparties, natural persons having a control of 25% or more in the company are identified. For clarity, a natural person is an individual who could be a shareholder or ultimate beneficial owner (UBO), power of attorney holder (POA), guarantor, signatory, or any other form of controlling stakeholder.

iv) To identify all the natural persons, the DPMS entity unwinds the legal structure to identify all the connected parties tracing them through any intermediate entities, until natural persons with ownership interests of 25% or more are identified. The DPMS entity uses the unwinding template to record all the connected parties (Appendix – 3).

v) The DPMS entity verifies the identity of any person legally empowered to act or transact business on behalf of the counterparty, whether the counterparty is a legal or natural person. Such persons may include:

- Nominees, signatories, or other authorized persons in case they are authorized to act on behalf of the customer.
- 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.
- If a legally empowered representative is also a legal person or Legal Arrangement, the normal CDD procedures for such entities are applied.

vi) UBOs are identified based on the UBO declaration to the licensing authority or as mentioned in the MOA or Board Resolution or any such legal documents.

vii) The identity of the person purporting to act on behalf of the counterparty is established through the any of the following set of documents.

- A legally valid power-of-attorney.
- A properly executed resolution of a legal person's or Legal Arrangement's governing board or committee (MOA, board resolution, etc.)
- 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.

viii) In case of Trust structures, the natural persons are the settlors, trustees and protectors. The DPMS entity duly identifies and verifies them through their identification documents.

ix) At the stage of identification and verification of the counterparty and all connected parties, if there are grounds for any suspicion due to any of the red-flag indicators given in appendix – 4, then the counterparty should be declined to be onboarded. The case should be escalated to the MLRO or Compliance Officer who in turn may investigate further and choose to file a Suspicious Activity Report (SAR) with Financial Intelligence Unit (FIU). Refer to TFS policies and procedures manual for further details. Counterparty declines are captured in a decline register (Appendix – 9) and periodically shared with senior management and MLRO / CO.

Confidential KHRYSOS TRADING DMCC

## 4.1. ID & Address verification of individuals & natural persons

In case of natural persons, the verification of a customer's identity, including their address, is verified based on original government-issued documents. The identification documents include,

- Photo of the individual or natural person
- Name, nationality, date of birth and place of birth,
- National identification number.
- Residence address

### *4.1.1. Verification of residents*

For verifying the identity of UAE nationals and UAE residents, copies of the following documents are obtained.

- Passport
- Emirates ID
- Family book (UAE nationals)

The customer facing staff of the DPMS entity verifies the copies against their originals and affixes his / her name, title, date, employee ID and signature along with the statement stating, "Original sighted". For residents the following set of documents are accepted for the purpose of address verification.

- Bills or account statements from public utilities (e.g., DEWA, SEWA, ADEWA, Du, Etisalat, etc.)
- Registered property purchase, lease or rental agreements
- Local and national government-issued documents, including municipal tax records.
- Documents from supervised third-party financial institutions, such as bank statements, credit or debit card statements, or insurance policies with address information
- An address verification letter from his / her previous employer can also be used (applicable only in cases where the person is unable to provide address verification as he / she is sharing their accommodation or yet to get their permanent address in the country)

### *4.1.2. Verification of non-residents*

In case of verifying foreign nationals, who are non-residents, their copies of passport and national ID should be obtained and certified by the DPMS entity's staff, if the non-resident client visits the DPMS entity or a staff member of the DPMS entity visits the counterparty's location. However, if the foreign national counterparty has not been visited in-person, then the following verification is applied.

- Attestation of identity documents from a notary public or lawyer or accountant is required.
- The attestation information contains 'True copy of the original', Verifying organization name, staff's name, title and signature.

In cases where documents are obtained from foreign sources in countries which are members of The Hague Apostille Convention, consideration can be given to requesting documents certified by Apostille seal. The official list of countries participated in Hague Apostille convention can be found in here (Hague Apostille Country List (gsccca.org)).

## 4.2. ID and Address verification of Legal entities

The entity obtains copies of following identity verification documents from legal entity clients.

- Trade license of the entity
- Certificate of incorporation
- Memorandum of Association (MoA)
- Board resolution reflecting change in company's structure.

CONFIDENTIAL KHRAM TRADING DMCC

- Share registry / certificate.
- Certificate of incumbency or good standing attested by the embassy or consulate in UAE (only for entities registered outside UAE)

These documents are verified against independent and reliable government sources.

### *4.2.1. Verification of locally registered entities (corporates or structures)*

The DPMS entity uses the National Economic Register to verify locally registered entities. Through the UAE's National Economic register (NER), businesses can view online their business licence details which the government has on record and get instant information about existing companies and business activities in the UAE. The registry can be accessed using the following link:

- ner.economy.ae/Search_By_BN.aspx

The link contains businesses licensed from the below authorities.

- Ministry of Economy
- Abu Dhabi Department of Economic Development
- Department of Economy and Tourism – Dubai
- Economic Development Department – Sharjah
- Department of Economic Development – Ras Al Khaimah
- Department of Economic Development – Ajman
- Department of Economic Development – Umm Al Quwain
- Fujairah Municipality
- Dibba Municipality (Arabic)

Wherever, 'eDocument Verification no.' has been mentioned in the copy of the Trade License, the firm inputs the same in the respective license issuing authority's portal. The firm takes a print screen of the output with date and time stamp and files it along with the other KYC documents of the client.

Wherever, the Trade License, has a reference to QR code verification, the same will be verified using user's mobile. While scanning the QR, the trade license will be opened on the mobile directly from regulator's website. The user who has done the verification should make a reference that the trade license has been verified using QR code and date and sign on the copy of the trade license.

### *4.2.2. Verification of foreign entities (corporates or structures)*

A foreign entity could be any of the following.

- Direct client of the DPMS entity
- Parent entity holding 25% or more stake in the DPMS entity's direct client.

In either of these cases, the natural persons holding controlling stake more than 25% in the counterparty of the DPMS entity are identified and verified (refer section 4.1). A counterparty who is a legal entity, is verified through the respective government's portal for verification of business registration numbers. While verifying the counterparty, personal details of the owners / shareholders are cross checked against counterparty declaration. In the absence of an independent government or regulatory portal for verification, the following approach is followed.

- Attestation of identity documents from a notary public or law firm or accountant is required.

- The attestation information contains 'True copy of the original', Verifying organization name, staff's name, title and signature.

Attestation is obtained for KYC documents of natural persons of the counterparty too.

Confidential - KAYROS TRADING DMCC

All connected parties related to the client viz. shareholders, UBOs, owners, guarantors, controlling stakeholders, parent companies with 25% or more controlling stake and subsidiaries (if more than 51% stake is held by DPMS entity's client), get screened for sanctions risk using UAE local list and UN consolidated list before proceeding to risk profiling the client (refer to TFS procedure manual for more details)

## 4.3. EXCEPTIONS TO IDENTIFICATION & VERIFICATION

Under the circumstances described below, the DPMS entity is permitted to handle the timing, customer identification, and other aspects of customer due diligence procedures exceptionally.

4.3.1. When there is no ML/FT suspicion, and the ML/FT risks are identified as low, the DPMS entity may complete the verification of the customer's identity after establishing the Business Relationship. However, these cases are tracked, and every attempt is made to complete the verification of the identity in a timely fashion. In any case, until the CDD procedures are completed no services are offered to the clients. This is applicable only to 'Simplified Due Diligence' clients (refer section on client risk profiling below)

4.3.2. While engaging clients / counterparties where contingent beneficiaries have been mentioned, then the DPMS entity obtains sufficient information about the details of the class of beneficiaries before engaging with the counterparty. Under no circumstances the DPMS entity provides its services to such counterparties whose contingent beneficiaries are from sanctioned countries.

4.3.3. For public listed companies, the DPMS entity is exempted from taking identify verifications measures of shareholders, UBOs, partners. The DPMS entity ensures that the disclosure and transparency requirements of the regulated stock exchange are at least equivalent to those of UAE. The DPMS entity is also exempted from taking identify verifications measures when the client, or the owner holding the controlling interest of the client, is a company listed on a regulated stock exchange subject to adequate disclosure and transparency requirements related to Beneficial Ownership; or when the client, or the owner holding the controlling interest of a legal entity client, is the majority-held subsidiary of such a listed company. While the above exemptions apply to shareholders & UBOs, the DPMS entity ascertains the identity of senior management through reliable information sources listed below.

- Stock exchange disclosure reports or websites
- Corporate annual reports, websites, or other forms of official public disclosure
- Official or public registries
- Credit reporting agencies
- Recognized, well-established media outlets.

4.3.4. When the DPMS entity suspects that a counterparty or UBO is involved in the commitment of a crime related to money laundering, the financing of terrorism, or the financing of illegal organisations, and there are reasonable grounds to believe that undertaking customer due diligence measures would tip off the client, then CDD measures are not applied. Instead, the case gets escalated to the Compliance Officer / MLRO, and a SAR gets filed with FIU along with the reasons that prevented the DPMS entity from carrying out the CDD measures.

4.3.5. Counterparties onboarded or services offered on an exception basis (e.g., with expired trade license, expired identification documents, etc.) are approved by senior manager with proper rationale. The instances are captured in the KYC / CDD exception management tracker (Appendix – 5) and all attempts are made to regularize such cases as early as possible. This is applicable only for 'Simplified Due Diligence' and 'Standard Due Diligence' clients (refer to counterparty risk profiling section below)

Confidential - KAMAL TRADING DMCC

**[BEFORE PROCEEDING FURTHER, SANCTIONS SCREENING IS PERFORMED FOR THE PROSPECT. REFER TO TFS PROCEDURE MANUAL FOR PROCESS STEPS & CONTROLS]**

## 4.4. Counterparty Risk Assessment

An accurate assessment of counterparty relationship risk is fundamental to the risk classification. Each counterparty's ML/FT risk profile is dynamic and subject to change depending on numerous factors. An appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified.

4.4.1. The DPMS entity analyses counterparties on the basis of the identified risk factors in order to arrive at a risk classification. A 'Counterparty Risk Assessment' template (CRA template) given in appendix – 1 is used for the purpose of profiling and classification.

4.4.2. CRA is completed for counterparties engaged in covered transactions.

4.4.3. When screening for adverse media news using open internet searches, the entity assesses the first 20 links for any adverse information. Wherever there are no adverse media news found against the client, the entity's staff comments as 'No Adverse Media News found' on the results page of the search. If some adverse news is found, then the staff performs a more detailed analysis before deciding whether to engage or decline the client.

4.4.4. If a decision to engage the client has been taken, then the rationale for the decision should be clearly documented either in the CRA template given in appendix -1 or on the results page of the internet search. Also file the relevant internet search pages and links along with the results page. If the decision is 'not to engage with the client', then update the client decline register given in appendix – 9

4.4.5. Similarly, while doing internet searches, if any political exposure (PEP) is noticed on the client or any of the natural persons, then the same should be further investigated. Should the PEP status be confirmed then apply EDD measures as discussed in relevant section below. If there is no PEP status noticed, then the entity's staff comments as 'No PEP found' on the results page of the search.

4.4.6. **Foreign Politically Exposed Persons (PEP) and Local PEP**: As part of Client Due Diligence, if PEPs are identified then the risk profile will be rated as High. As per the CDD risk assessment, a PEP warrants a mandatory EDD (Enhanced Due Diligence) and EDD measures are applied as per section 4.5.2 of the procedure manual. However, in case of local PEP the measure differs from foreign PEPs.

In case of foreign PEP, the controls as stipulated in 4.5.2 will be applied. However, for local PEPs, the adverse media checks using open internet searches will be performed. In the event, any adverse media allegations are noted against local PEPs, then bank statements will be obtained. As part of open internet searches, if positive news items are found (e.g., awards received from the president of the country), then the EDD measures will be relaxed for such clients.

4.4.7. In the case of legal structures, CRA is completed for each of the natural persons holding 25% or more stake in the counterparty. Natural persons are listed below.

- Shareholders

Confidential - KINGS TRADING DMCC

- Nominees
- UBOs
- POAs
- Signatories
- Guarantors
- Any other controlling stake holders (mandatory requirement to profile anyone controlling more than 25%)

4.4.8. The risk factors used to assess client's ML/FT risk profile are as follows:

| Risk factor | Variables analyzed |
|---|---|
| ***Counterparty risk*** | Ease of ID verification, net worth of individual, complexity of structure, transparency of UBOs, association with high-risk persons (political exposure, adverse news), use of cash or virtual assets to settle the transaction, Knowledge, expertise, technical and financial capacity |
| ***Geographic risk*** | Stronger or weaker regulatory and supervisory framework in client's country of residence, principal residential or operating locations of customers, high risk countries as per FATF, tax haven countries |
| ***Product & services risk / Transaction risk*** | Client's line of business, industry type, complexity of products & services offered to customers, if the property is used by self or for investment purposes, engaged in a covered or a non-covered transaction |
| ***Delivery channel risk*** | Favors anonymity during client acquisition, business relationship or service delivery. |

4.4.9. In the following circumstances the counterparty gets mandatorily classified as EDD

- If a legal entity counterparty is registered in or predominantly operates from a FATF blacklist country (Iran, Myanmar and North Korea). In the case of individuals / natural persons if the person is a resides in one of the FATF blacklisted countries. The blacklisted countries can be referred to in the below link.

  High-Risk Jurisdictions subject to a Call for Action - October 2023 (fatf-gafi.org)

- PEP (relatives and friends) – Applies to individuals and natural persons like shareholders, UBOs, POAs or other controllers of the legal entity. If any of the natural persons are found to be a PEP, then the Company is EDD.
- Adverse media news on individual or legal entity counterparty or any natural persons holding 25% or more stake in the legal entity (after qualifying the adverse information)
- Complex structures (natural person with 25% or more stakes exists 3 layers above the counterparty)
- If any connected party of a counterparty is classified as EDD, then classify the legal entity as EDD.

4.4.10. The DPMS entity identifies PEPs based on the below identifiers:

- Politicians,
- Current and ex-ministers,
- Senior managers in government departments or quasi government organizations,
- Judiciary or military officials
- Have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation.
- Direct family members of PEP (spouses, children, spouses of children, parents)

Confidential - KHRYSOS FZ LLC DMCC

- 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 favour of the PEP.

Even if the above criteria may not be applicable at the time of onboarding or periodic review, prior 5 years records are considered before applying non-PEP status.

4.4.11. The DPMS entity maintains a PEP register which documents all the PEPs and their KYC and CDD details (refer to Appendix – 6).

4.4.12. For counterparties who are not mandatorily classified as EDD, a risk score is applied for each of the risk factors in the CRA template.

***Risk scoring for legal entity counterparties is based on the following criteria:***

1) A counterparty is a single legal entity or part of a larger / complex group.
2) Counterparty's knowledge, expertise, financial and technical capability in PMS transaction.
3) Clarity on the income of the legal entity and reasonableness of the wealth
4) Nature of counterparty's business activity:
   - Is the company engaged in normal business activities or used only for investments in property or financial products?
   - Business activities of the company, parent, subsidiaries (e.g., real estate, precious metals, UAE controlled list, Dual Use goods, etc.)
5) Frequency of covered transactions.
6) Counterparty referred by existing client or referred by 3rd party referral or acquired through sales team.
7) Interaction with the natural persons connected with the counterparty is face to face or non-face-to-face.
8) Counterparty (registered in UAE) or its subsidiary has business dealing with high-risk countries (as defined by FATF) or with tax haven countries.
9) Counterparty is registered outside UAE.

Scoring points 8 & 9 related to country risk are scored based on the ratings table published in 'knowyourcountry.com'. Consideration has been given to ML/TF risks, international sanctions, corruption risk, global initiative criminality index, global initiative resilience index, EU tax blacklist and offshore finance centre. The ratings table is accessed using the below link:

Ratings Table – KnowYourCountry

***Risk scoring for individuals and natural persons are based on the following criteria:***

1) Ease of obtaining and verifying ID documents and Address proof documents from the natural persons
2) Retail client's / Counterparty's knowledge, experience, financial and technical capability
3) Net worth of natural persons or individuals (high net worth is considered as more than AED 3.6 million)
4) An individual or natural person is a key decision maker in the company that operates in an industry with high AML risk (controlled items, Dual Use Goods, chemicals)
5) Frequency of covered transactions
6) Interaction with the individual / natural person is face to face or non-face-to-face.
7) A UAE resident whose nationality is from high-risk jurisdiction or tax haven country.
8) Non-UAE resident's residency status is from high-risk jurisdiction or tax haven country.

Scoring points 7 & 8 related to country risk are scored based on the ratings table published in 'knowyourcountry.com'. Consideration has been given to ML/TF risks, international sanctions, corruption risk, global initiative criminality index, global initiative resilience index, EU tax blacklist and offshore finance centre. The ratings table is accessed using the below link:

Confidential KNOWSOMORE DMCC

Ratings Table – KnowYourCountry

4.4.13. Rationale for exceptions to the risk scoring of clients are captured in the notes section of the CRA form and signed off by Senior Management of the DPMS entity.

4.4.14. PEP and Adverse media are identified through the screening tool used by the entity. Further, to complement the screening tool, the DPMS entity uses an open internet search to verify the client's PEP status and to validate any Adverse media news.

4.4.15. After risk scoring the natural persons, risk classification details of the counterparty are captured in the client risk classification register (Appendix – 12)

## 4.5. Enhanced Due Diligence (EDD)

The DPMS entity applies Enhanced Due Diligence for all counterparties engaging in covered transactions based on either mandatory EDD or whose risk profile has been identified as 'High' as per the CDD risk profiling form. EDD involves a more rigorous application of CDD measures as follows:

- Customer identity:
  - Increased scrutiny and higher standards of verification and documentation from reliable and independent sources
- More detailed inquiry and evaluation of reasonableness regarding the,
  - Purpose of the Business Relationship
  - Nature of the customer's business
  - Customer's source of funds and source of wealth, and
  - Purpose of individual transactions
- Increased supervision of the Business Relationship, including
  - Requirement for higher levels of management approval,
  - More frequent monitoring of transactions, and
  - More frequent review and updating of customer due diligence information.

4.1.1. If the EDD leads to the fact that the counterparty is engaged in the following activities, then the DPMS entity does not enter into a business relationship:

- Fraud
- Counterfeiting and piracy of products
- Illicit trafficking in narcotics,
- Providing professional third-party money laundering services
- Insider trading and market manipulation
- Robbery and theft
- Illicit arms dealer
- Forgery
- Smuggling
- Tax crimes
- Dealing in UAE control list without a valid license
- Issues or is authorized to issue bearer shares.

When the above instances are noticed, the staff member of the DPMS entity escalates the same to Compliance Officer or MLRO who raises a SAR with FIU's goAML platform (refer to the TFS process manual for SAR procedures).

4.1.2. Following are the EDD measures applied by the DPMS entity.

a) Obtains and corroborates additional KYC information about the counterparty (e.g., occupation details, asset details) relating to the counterparty and the natural persons, where necessary. As an example, requesting the passport copy in cases where the counterparty has only

Confidential - KHK GOLD TRADING DMCC

provided a national ID document (for individuals), or requesting the memorandum of association (MOA) in cases where the counterparty has only provided the trade license (for entities)

b) Further, manual internet searches are performed for more detailed background checks like foreign PEP, adverse information, etc.

c) Obtains a source of funds or source of wealth (any one of the following) to check if income is in line with the nature of business & size of its operations.
   - Bank statement for 3 months prior to the date of the transaction or a banking reference letter (for individual or corporate counterparties)
   - Reference letter from an auditor (for corporate counterparties)
   - Audited financial statements (for corporate counterparties)

d) Applies the following Transaction Monitoring criteria:
   - As a general principle, the red-flags as stipulated by the regulatory guidelines and captured in Appendix-4 of this documents are monitored for all the counterparties. More specifically, undue urgency shown by the counterparty in closing the deal and evasiveness in providing necessary information.
   - For EDD counterparties with whom the DPMS entity has an ongoing business relationship (suppliers of the DPMS entity or retail stores supplied by the DPMS entity), in addition to red flags, the following also gets monitored.
     - Screening for sanctions and PEP on a monthly basis
     - On an annual basis, entire CDD is reperformed (refer to section on Periodic Review below)

e) In case of covered transactions, maintaining careful records of the certificate numbers and/or identifying characteristics (including weight, purity/quality, colour, shape, cut, inclusions or other markings, and other relevant factors).

f) Applies the following ongoing screening criteria for Targeted Financial Sanctions (UN consolidated list and UAE terrorist list):
   - *Corporate counterparty:*
     i) Screen top 3 suppliers and top 3 customers of the counterparty
     ii) Monthly screening performed for a period of six months post termination of the business relationship.

   - *Individual counterparty:*
     i) Monthly screening performed for a period of six months post termination of the business relationship.

g) If the PEP is foreign, then the full ED measure is applied. In case of local PEP, MLRO judgement is allowed on the extend of applicable EDD measures. For example, based on additional open internet searches if there are positive news regarding the local PEP, like award from the president, etc. then a lenient EDD measure will be applied.

h) All EDD cases are approved by Senior Management of the DPMS entity before onboarding and during each CDD cycle (once a year) or whenever it gets triggered (refer to trigger event reviews section below)

4.1.3. While dealing with Non-Profit Organizations (NPO), the DPMS entity ensures that the client is properly licensed or registered and obtains sufficient information regarding regulatory disclosure requirements, accounting, financial reporting and statutory audit report. EDD measures are applied on the NPO's key persons, such as senior management, branch or field managers, major donors and major beneficiaries.

4.1.4. At any stage, while performing CDD, the DPMS entity checks for any of the red-flag indicators as provided in appendix – 4. In case red flags are identified, then the matter is immediately escalated to MLRO / Compliance Officer. After making preliminary investigations, if there is ground for suspicion, then the matter is reported to FIU through the goAML portal (refer to TFS policies and procedures manual)

Confidential - KIRTOS TRADING DMCC

## 4.6. Simplified Due Diligence (SDD)

SDD generally involves a more lenient application of certain aspects of CDD measures, including elements as:

- A reduction in verification requirements regarding customer or Beneficial Owner identification
- Fewer and less detailed inquiries regarding 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.

Though the DPMS client may open a business relationship with the counterparty, before verification of ID documents, the identification documents are obtained and verified before the deal gets completed.

## 4.7. Transaction Monitoring (TM)

Due to the transactional nature of its relationship with the client, the DPMS entity has limited access to the client's financial transactions posing challenges to ongoing monitoring. Transaction Monitoring (TM) is applied on the counterparties with whom the DPMS entity has an ongoing business relationship either in the supply side (wholesale intermediary supplying PMS goods to the DPMS entity) or the sales side (other retail or wholesale intermediary dealing in PMS goods).

The DPMS entity closely monitors red-flag indicators given in appendix - 4 (behavioral, structural or transactional in nature) during the entire life cycle of the engagement and immediately escalates such cases to Compliance Officer / MLRO for further action (refer to TFS manual for SAR process).

Further, transactions are always monitored for covered or non-covered transactions (list of covered transactions are given in section 4 related to CDD). Covered transactions could be identified either before executing a transaction or after executing a transaction i.e., as part of post transactional review. Covered transactions are reported in goAML using the DPMSR option.

## 4.8. Trigger event reviews (TE)

Any event that warrants a re-assessment of a counterparty's AML risk profile is covered under Trigger Event Review. As part of the reassessment, the CDD procedures in its entirety is applied when the following are noticed (list is non-exhaustive).

- Change in corporate headquarters.
- Change in beneficial owner.
- Change in legal name of the counterparty.
- Change in the corporate structure or the counterparty.
- Changes in guarantors or ownership (e.g., death, buyout).
- A change in the person conducting transactions for a business customer.
- A change identified during periodic reviews of high-risk customers (e.g., non-PEP becoming a PEP, a qualified adverse media news, involvement in fraud or drugs, etc.).

The events above are used to assess the documentation held by the DPMS entity. Upon identification of a trigger event the following activities are considered on a case-to-case basis.

- An assessment of risk
- Does the due diligence already performed still meet requirements?
- Does it need to be refreshed?
- Is enhanced due diligence required?
- Has the event led to suspicion?

## 4.9. Periodic Reviews

Most of the deals of the DPMS entity are transactional in nature i.e., one-off transaction. AML/CFT procedures in its entirety is applied for all covered transactions.

Periodic reviews are applied by the DPMS entity where it has ongoing business relationship with its suppliers (or other retail businesses, where and when applicable). Following is the periodic review cycle followed by the DPMS entity based on the counterparty's risk rating.

| | |
|---|---|
| Counterparties classified as Simplified and Standard Due Diligence | Periodic review is done once every 3 years |
| Counterparties classified as Enhanced Due Diligence | Periodic review is done once every year |

During each periodic reviews, fresh set of CDD documents are obtained from the counterparties and risk profiling is done using the CRA template. CRA templates used for each of the counterparties are retained as per the record retention policy discussed in the below section.

## 4.10. Reliance on a Third Party

The DPMS entity may in future rely on third parties to fulfil its CDD obligations by ensuring that the third parties are regulated and supervised and adheres to the CDD measures towards customers and record-keeping provisions stipulated by "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions".

4.10.1. While engaging third parties, the DPMS entity would sign a clearly defined agreement with the senior management of the third party. Before signing the agreement, the DPMS entity would evaluate the third party for its comprehensiveness and quality of its AML/CFT policies, procedures and controls; the number of personnel dedicated to CDD; and its audit and/or quality assurance policies regarding CDD.

4.10.2. The agreement would have provision to incorporate questionnaires, scorecards, and on-site visits to evaluate the adequacy of a third party's adherence. Service-level agreements with the third party would clearly set out the roles and responsibilities of the DPMS entity and the third party and specifying the nature of the CDD and record-keeping requirements to be fulfilled.

4.10.3. If engaging foreign third parties, the DPMS entity will ensure that the 3rd party strictly adheres to the AML/CFT requirements as per UAE requirements. The agreement would obligate the third party to submit the copies of identification data and other relevant documentation relating to the CDD requirements to the DPMS entity upon request without delay. The DPMS entity obtains evidence of the third party's regulatory and supervisory status and good standing, and they would also consider obtaining the third party's certification that any CDD documents provided by them (such as identification documents, proof of address, or documents corroborating a customer's source of funds) are true copies of the originals.

Confidential - HURRY TRADING DMCC

# 5. GOVERNANCE

## 5.1. COMPLIANCE OFFICER:

Following is the contact details of the Compliance Officer (CO) of the DPMS entity:

Name : Rajesh Kumar

Email : ceo@khrysosdmcc.com

Phone1 : +971 50 900 1975

5.1.1. The CO acts on his own authority and has direct access to the senior management and the Legal Authority of the UAE. He has sufficient resources to assist in the performance of his duties in an effective, objective and independent manner; and has unrestricted access to information about all the clients and more specifically on those potentially involved or suspected to be involved in money laundering activities.

5.1.2. The designated CO of the DPMS entity has been assigned with the following responsibilities:

- Establish and maintain the DPMS entity's anti money laundering policies, procedures, systems and controls and compliance with anti-money laundering legislation applicable in the UAE.
- Challenges decisions that are ill-suited and protect the DPMS entity from potential ML/FT abuse.
- Keep a close watch on EDD clients while onboarding, periodic reviews and trigger event reviews.
- Act as a point of contact to receive internal Suspicious Transaction / Activity Reports from the DPMS entity's employees.
- Table semi-annual AML reports to the senior management and wherever mandatory to the relevant Supervisory Authorities.
- Inform and report to senior management on the level of compliance and report on that to the relevant Supervisory Authority.
- Assess the impact of new policies and procedures on the DPMS entity's existing AML/CFT framework and wherever necessary make amendments to the procedure manual and retrain the staff.
- Take appropriate action following the receipt of an internal Suspicious Transaction / Activity Report from the employees and reporting to the Financial Intelligence Unit (FIU) of the UAE (or to the relevant authorities like DFSA)
- Act as a point of contact within the DPMS entity for the regulators regarding money laundering issues
- Establish and maintain a strong and effective AML/CFT compliance culture within the DPMS entity. This duty includes working with senior management and other internal and external stakeholders to ensure that the DPMS entity's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.
- Submit semi-annual AML report to the management (Appendix 13)

The responsibilities of the Compliance Officer are captured in the Job Description in Appendix 14.

5.1.3. If the DPMS entity decides to appoint a MLRO, then his / her responsibility would be to assist the CO in the above-mentioned responsibilities. The reporting structure of the CO is given in appendix – 7.

5.1.4. Due to the small size of the DPMS entity, from time to time, the above-mentioned CO responsibilities may be performed by a member of staff who is also engaged in managing

Confidential KHRYSOS TRADING LLC

counterparty relationship. This may result in conflict of the incumbents CO responsibilities. As a mitigant, the DPMS entity conducts a Quality Assurance (QA) by an internal staff independent to the entire CDD process or by an external consultant once every 6 months.

5.1.5. The QA is further complemented with an external audit program. The first audit will be conducted 1 year after implementation of this new procedure.

## 5.2. Training And Staff Screening

The DPMS entity provides periodic information and training to all employees to ensure that they are aware of the following information pertaining to AML / CFT.

- Identity and responsibilities of the DPMS entity's CO.
- Applicable legislation relating to anti money laundering.
- Potential effect on the DPMS entity, its employees, and its counterparties of breaches of applicable legislation relating to money laundering.
- DPMS entity's anti money laundering policies, procedures, systems and controls and any changes to these.
- Money laundering risks, trends and techniques.
- Types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged that may warrant an internal Suspicious Transaction Report.
- DPMS entity's arrangements regarding the making of an internal Suspicious Activity Report (SAR)

All relevant details of the DPMS entity's anti money laundering trainings are recorded in the training log (Appendix – 8), including:

- Dates when the training was given.
- Nature of the training, and
- Names of the Employees who received the training.
- Name of the trainer

The DPMS entity maintains screening records as part of background verification for all its staff members.

## 5.3. Quality Assurance (QA)

The DPMS entity conducts a QA on a semi-annual basis to check the operating effectiveness of the AML/CFT controls defined in this procedure manual. The scope of the QA covers the following aspects.

- Onboarding (KYC forms, KYC documents, unwinding template, screening results, counterparty risk profiling, risk classification and approvals wherever necessary)
- Ongoing screening, transaction monitoring including red-flags and trigger events during service delivery.
- Following registers and trackers maintained by the DPMS entity.
  - Client risk classification register
  - KYC / CDD exceptions tracker
  - PEP register
  - AML training log
  - Counterparty decline register
  - Counterparty exit register.
  - AML communications register
- Adherence to record retention policy.

The QA activity may be conducted either by a staff member independent to the AML / CFT procedures of the DPMS entity or may be outsourced to a third-party consultant with adequate knowledge regarding AML/CFT regulations of UAE.

Confidential KHRYSOS TRADING DMCC

## 5.4. Independent Audit

The DPMS entity appoints a third party to conduct and audit of its AML / CFT process and controls.

The audit will review the AML / CFT procedure of the DPMS entity to ascertain the control design effectiveness (CDE) and control operating effectiveness (COE).

The scope of the audits covers the following aspects:

- Examine the adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.
- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity.

Sampling for audit reviews include new counterparties, existing counterparties, ongoing engagements, one-off transactions, SDD files, EDD files, PEPs, Complex structures, counterparties where there is a change in ownership and/or nature of activities, etc.
After the first audit subsequent audits will be conducted once every 2 years and a detailed report of findings will be made available to the DPMS entity. The findings from the audit report are acted upon immediately to mitigate any identified risks. In case there are no High or Medium risk findings during the audit, then the senior management can increase the frequency of audit to 3 years.
However, the DPMS entity increases the frequency of audit to annually, if the CO is not independent of sales or client relationship management function.

## 5.5. Cash Acceptance Procedure

The entity monitors its payments closely and encourages non-cash / non-virtual asset-based transactions. In the event of accepting cash or virtual assets, following controls should be adopted.

| Sl. No | Cash limit | Approval matrix |
|---|---|---|
| 1 | Cash below AED 5000 | No specific approval required |
| 2 | Cash above AED 5000 and below AED 55000 | Approval from senior management |
| 3 | Cash above AED 55000 | Approval from senior management and MLRO<br><br>**Note:**<br>DPMSR to be raised in goAML |

Cash will be accepted only in the following instances:

- Client is in the process of getting a bank account opened in UAE
- Full Client Due Diligence (CDD) is done and as per the CDD risk assessment, client's risk rating is not Enhanced Due Diligence (EDD).
- Under no circumstance, virtual assets are accepted as a mode of settlement.

Wherever cash above AED 55,000 is accepted, the source of fund will be validated from the client.

Confidential - CHRYSOS TRADING DMCC

# 6. RECORD RETENTION

All relevant information, correspondence and documentation used by the DPMS entity to verify a counterparty's identity; and in respect of the ongoing due diligence and scrutiny, are kept for **at least five (5) years** from the date of completion of the transaction or in case of ongoing engagements, for 5 years after termination of the engagement.

Adherence to the record retention policy is validated during the independent QA.

A brief list of documents is given below, however, there could be other documents that may be used in conjunction with these. Such documents are also retained for a period of 5 years as per regulation.

| Process category | Documents |
|---|---|
| Onboarding | • KYC application form (signed by clients)<br>• ID documents along with verification details of clients, Beneficial Owners, shareholders, nominee shareholders, directors and 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 verified as part of onboarding.<br>• Screening results<br>• External open searches, reports from external service providers<br>• CDD risk profile template<br>• Client acceptance document including senior manager signoff for EDD clients.<br>• Source of wealth & Source of funds of clients<br>• Bank statements, reference letters<br>• All documents collected from clients as part of onboarding.<br>• Copies of SPA, SAA, MOU and rental agreement.<br>• Documents pertaining to red flag indicators.<br>• Client specific communication with regulators (e.g., proliferation goods checking with EOCN) |
| Periodic reviews & Trigger event reviews | • ID documents along with verification details of clients, Beneficial Owners, shareholders, nominee shareholders, directors and 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 verified as part of periodic review.<br>• Screening results<br>• External open searches, reports from external service providers<br>• CDD risk profile template<br>• Information pertaining to trigger event.<br>• All documents collected from clients as part of the review.<br>• External open searches, reports from external service providers during the reviews<br>• Client specific communication with regulators (e.g., proliferation goods checking with EOCN) |
| Transaction processing (or) transaction monitoring | • Client instructions or communications related to initiation of a transaction or service (e.g., documents related to account services, tax return filing, advisory, etc.)<br>• Transaction details pertaining to red flag indicators.<br>• Communication with client on red flag clarification<br>• Samples chosen while performing external or internal audit for clients.<br>• Suspicious activity escalated to MLRO / Compliance officer. |

Confidential

| Process category | Documents |
|---|---|
| | • All documents pertaining to investigating a potential SAR including communication with regulators if any.<br>• Closure of internal SAR<br>• SAR filed with FIU |
| Trackers / registers | • CDD exception tracker<br>• PEP register<br>• KCY documents renewal tracker<br>• SAR register<br>• Training register |
| General documents | • Business Risk Assessment<br>• Risk Assessment Matrix & Control Assessment Matrix<br>• Obligations register against applicable laws and regulations.<br>• Impact assessment carried out against new regulations.<br>• Self-assessment carried out against thematic review reports issued by regulators.<br>• Reports issued to clients.<br>• Any form of communication held with client (emails, physical letters or communications, etc.)<br>• Mails received from EOCN (especially list update related mails)<br>• Submissions to regulators (semi-annual reports, samples provided during regulatory reviews or used for internal audit)<br>• Reports received from regulators, auditors.<br>• Policies and procedures (current as well as for the last 5 years)<br>• Minutes of formal internal governance meetings along with MIS tabled in such meetings.<br>• 3rd party engagement contracts, SLAs, MIS received from 3rd parties, contract termination, etc.<br>• Minutes of formal meetings held with 3rd parties.<br>• Organisational roles and responsibilities for the implementation of service-level agreements with third parties governing the provision of record-keeping services.<br>• 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.<br>• Appropriate audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework.<br>• Appropriate audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework.<br>• All training materials used for staff training and training records.<br>• DPMS entity's own trade license copies and ID documents of partners, shareholders, beneficiaries, UBOs.<br>• DPMS entity's organization structure and variations to the structure<br>• DPMS entity's own MOA, board meeting minutes<br>• DPMS entity's own book of accounts<br>• Invoices sent to clients and received from vendors.<br>• Payment receipts given to clients or received from vendors.<br>• Letters issued to employees (appointment letters, labour contracts, warning letters, HR letters, Job descriptions, performance appraisals, etc.) |

Confidential – Property of DMCC

# LIST OF APPENDICES



Confidential - KHRYSOS TRADING DMCC