AML & CFT Policy

VERSION CONTROL

	Who
Owner Entity	KRYPTO BROKER INVEST
Domain	AML Risk & Compliance
Topic	KRYPTO BROKER INVEST AML & CFT Policy
Policy Owner	(CCO) Gulzhanat Shingisova, (MLRO) Alaa Shadid
Effective Date	1st May 2025
Revision Date	1st May 2026
Version	V1

Contents

1. INTRODUCTION

KRYPTO BROKER INVEST (the "Company") is dedicated to complying with all relevant anti-money laundering and counter-financing of terrorism (AML/CFT) laws and regulations. This policy includes measures to combat money laundering and terrorist financing, ensuring staff awareness of their obligations.

For onboarding clients, the Company follows its own KYC/AML policy, which may involve outsourcing to qualified vendors.

This Policy ensures compliance with UAE laws, UN Security Council Resolutions on terrorism, and related directives, as well as economic sanctions.

KRYPTO BROKER INVEST adheres to guidelines from VARA, UAE federal bodies, and the Financial Action Task Force (FATF).

All directors, officers, staff, and representatives must comply with this policy as a condition of their employment and sign the Staff AML/CFT Acknowledgement Form (attached as Annex C)

2. REGULATORY OBLIGATIONS

This policy refers to guidelines and recommendations from FATF, UAE laws, and the UAE Executive Office for Control and Non-Proliferation (EOCN).

2.1. Financial Action Task Force

The FATF updated its recommendations in June 2019, focusing on managing risks from virtual assets (VAS). Recommendation 15 advises countries to assess risks in the VAs industry and regulate Virtual Asset Service Providers (VASPs).

Recommendation 16 aims to prevent criminal access to wire transfers for illicit funds. It requires originating and beneficiary VASPs to obtain and securely share accurate information on virtual asset transfers with authorities when needed. Financial institutions must also comply with these obligations.

FATF has published reviews on the revised standards for VAs and VASPs, emphasizing the importance of implementing the Travel Rule and other AML/CFT obligations.

FATF's updated guidance provides insights into applying standards to stable coins, peer-to-peer transactions, and licensing VASPs.

KRYPTO BROKER INVEST commits to complying with FATF recommendations to combat money laundering and terrorist financing.

2.2. United Arab Emirates Laws and Legislations

In the United Arab Emirates ("UAE"), the following legislations and guidelines are applicable and useful for reference.

- Federal Decree No. 20 of 2018 on AML/CFT Federal Decree No. 20 of 2018 was issued to develop the legislative and legal structure of the nation to ensure compliance with international standards on anti-money laundering and countering the financing of terrorism. The law aims to:
  - Combat money-laundering practices.
  - Establish a legal framework that supports the authorities concerned with anti-money laundering and crimes related to money-laundering.
  - Counter the financing of terrorist operations and suspicious organisations.
- The Federal Law No. 4 Concerning the Emirates Securities and Commodities Authority and Market, as amended Securities and Commodities Authority ("SCA") was formed to strengthen the legislative structure through issuing regulations and instructions that ensure the development of the organisational and supervisory framework of the listed joint-stock companies and other companies operating in the securities market licensed by SCA across the UAE. Regulations specific to virtual assets are as follows:
  - The Federal Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (Virtual Assets Law) was published in the Official Gazette of the Government of Dubai. The Law empowers Dubai Virtual Assets Regulatory Authority (VARA) in charge of regulating, licensing, supervising, and overseeing Virtual Asset services in the Emirate.
  - The applicable law, rules and regulations governing anti-money laundering and countering terrorist financing activities in the UAE are as listed below:
    - Federal Law No. 4 of 2002 concerning the Criminalization of Money Laundering.
    - Federal Law No. 9 of 2014 amending certain provisions of Federal Law No. 4 of 2002 concerning the Combating of Money Laundering Crime.
    - Cabinet Resolution No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018.
    - Cabinet Resolution No. 38 of 2014 Concerning the Executive Regulation of the Federal Law No. 4 of 2002 Concerning Anti Money Laundering and Combating Terrorism Financing.
    - Cabinet Decision No. 74 Regarding Terrorism Lists Regulation and implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions.
    - Federal Law No. 7 of 2014 regarding Combating Terrorist Offences.
    - The Penal Code of the United Arab Emirates.

2.3. UAE Executive Office for Control and Non-Proliferation (EOCN)

The EOCN has provided guidance on Counter Proliferation Financing for Financial Institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs), and VASPs. This guidance clarifies the UAE's AML/CFT framework concerning proliferation financing and includes a list for identifying and addressing sanctions evasion activities related to proliferation financing.

KRYPTO BROKER INVEST will adhere to the EOCN's local Terrorist List and any subsequent amendments.

3. AML/CFT MEASURES

To ensure effective implementation of AML/CFT policies, KRYPTO BROKER INVEST has established the following measures to comply with all relevant laws and regulations:

- **Client Screening:** Risk rules are in place to screen clients, beneficial owners, VA transactions, and wallet addresses for potential illicit activities and applicable sanctions, alerting compliance teams for further investigation.
- **Regular Reviews:** Procedures ensure ongoing evaluation of distributed ledger analytic tools and monitoring of client interactions with VA activities.
- **Internal Controls:** Controls are implemented to address FATF's Virtual Assets Red Flags when designing transaction monitoring scenarios.
- **Third-Party Attestation:** This policy must be verified by a competent third party, and results submitted to VARA.
- **Compliance Officer (CO):** A senior management-level CO is appointed to oversee the AML/CFT systems.
- **Money Laundering Reporting Officer (MLRO):** A senior staff member is designated as MLRO to manage suspicious transaction reports, with annual reviews.
- **Qualifications:** Both the CO and MLRO must be fit and proper persons, with the CO residing in the UAE.
- **Multiple Roles:** The CO may hold non-client-facing roles within KRYPTO BROKER INVEST, provided there are no conflicting duties, subject to VARA approval.
- **VA Transactions** - Krypto Broker ensures compliance with Virtual Asset transaction regulations by continuously assessing AML/CFT risk management policies and internal controls, tailored to each client's risk profile and transaction.
- **FATF** - In line with the FATF Report on Virtual Assets Red Flags for Money Laundering and Terrorist Financing, Krypto Brokers Compliance and Risk teams collaborate with IT and data analytics to implement effective risk mitigation systems across all VA-related activities, including analytics, sanctions screening, and anomaly detection.

3.1. Roles and Responsibilities

3.1.1. Compliance Officer

The Compliance Officer's responsibilities include:

- Disseminating updates on money laundering and terrorist financing regulations to staff.
- Monitoring and testing AML/CFT policies, procedures, and controls.
- Identifying and addressing deficiencies in AML/CFT systems.
- Mitigating ML/TF risks from business relationships with high-risk countries.
- Communicating key AML/CFT issues and significant compliance deficiencies to senior management.
- Ensuring staff adherence to policies and procedures.
- Providing or arranging training on anti-money laundering and counter-terrorist financing.

3.1.2. MLRO

The MLRO's responsibilities include:

- Conducting regular independent reviews of client transactions to identify suspicious activities.
- Analyzing and investigating suspicious transactions reported by staff.
- Reporting suspicious transactions to local authorities, such as the Financial Intelligence Unit of the UAE Central Bank.
- Monitoring regulatory developments and implementing AML/CFT policies and procedures.
- Conducting AML/CFT risk assessments and updating relevant policies as needed.
- Ensuring quarterly reports include summaries of Anonymity-Enhanced Transactions and involved clients.
- Maintaining a register of all reports made to the authorities and the reasons for them.
- Providing guidance to avoid "tipping off" in cases of suspected money laundering.
- Serving as the main contact with authorities regarding AML/CFT matters and reporting to VARA as required.
- Reporting quarterly to the Board on the status of the AML/CFT program, including any compliance breaches.
- Overseeing corrective actions in response to compliance breaches with federal AML/CFT laws.
- Providing training to all staff, including board members, on AML/CFT laws and requirements.
- Being responsible for the implementation of the AML/CFT program and overseeing any outsourced arrangements.

3.1.3. Company staff

The responsibilities of the Company staff are to:

- Follow the policies and procedures to ensure appropriate measures are incorporated to prevent money laundering and terrorist financing.
- Be aware of and comply with relevant legislation and guideline; and
- Cooperate with the relevant law enforcement authorities, including timely disclosure of information.

4. CUSTOMER DUE DILIGENCE ("CDD")

KRYPTO BROKER INVEST must perform Customer Due Diligence (CDD) in the following situations:

- When establishing a business relationship for VA services.
- For occasional transactions of AED 3,500 or more, whether single or linked.
- Upon client instructions regarding potential suspicious transactions.
- If there are doubts about previously obtained identification information.
- For transactions involving high-risk clients as defined by federal AML/CFT laws.
-

Anonymous or fictitious accounts are prohibited. For joint accounts, CDD must be performed on all holders as if they were individual clients.

If CDD cannot be completed, KRYPTO BROKER INVEST will not:

- Establish or maintain a business relationship.
- Execute any transactions for that client.
-

When relying on third parties for CDD, KRYPTO BROKER INVEST remains responsible for their actions and must ensure compliance with applicable laws. Adequate controls will be implemented to monitor third-party performance in relation to business changes.

4.1. Natural persons (“individual clients”)

At a minimum, KRYPTO BROKER INVEST must obtain the following information:

- Full name as per identification (including a copy of the ID or travel document)
- Date of birth
- Place of birth
- Nationality
- Unique identification number (e.g., ID card or passport number) and document type
- Residential address (verified by ID, recent utility bill, bank statement, or government correspondence; a P.O. box may be accepted where applicable)
- Contact details (personal, office, or work phone numbers)

- Source of funds (e.g., savings, employment income)
- Confirmation of any prominent public function held by the customer
- Identification of the beneficial owner if the customer is not the account holder.

KRYPTO BROKER INVEST must also verify this information using reliable, independent sources, such as government-issued IDs or independent documents. Copies of identification documents should be maintained per the record-keeping policy.

4.2. Corporates, businesses, and trusts ("non-individual clients")

At a minimum, the following information must be obtained:

- Full registered business name, including any aliases.
- Nature of business and type of entity
- Legal form and governing regulations
- Date of establishment or registration
- For trusts, the governing jurisdiction
- Place of incorporation or registration
- Unique identification number (e.g., business registration or tax ID)
- Address of the registered office
- Principal place of business address
- Ownership and control structure (signed by directors or authorized personnel)
- Locations of headquarters, operating facilities, branches, and subsidiaries
- Source of funds
- Board resolution authorizing account opening and signatory authority.
- Constitutional documents (e.g., memorandum and articles of association) attested by UAE authorities.
- Names of individuals in senior management positions
- If the client or UBO is a Politically Exposed Person (PEP), approval from the MLRO and senior management is required before establishing a business relationship.
- Verification of any entity acting on behalf of the client as per VARA Compliance and Risk management rulebook Rule III.E.5
- Understanding the intended purpose of the business relationship and obtaining relevant information
- For business clients, understanding their nature and ownership structure.
- Verification of beneficial owners (BOs) and ultimate beneficial owners (UBOs)
- Identification of any Decentralized Autonomous Organizations (DAOs) involved and their intended purpose.
- Due diligence on the client's clientele to ensure compliance with federal AML/CFT laws.

4.3. Beneficial Owner

For a corporate entity or partnership, a beneficial owner is an individual who:

- Owns or controls 25% or more of the issued share capital or profits, directly or indirectly (including through trusts or bearer shares).
- Controls 25% or more of the voting rights at general meetings.
- Exercises ultimate control over the corporation's management or represents another person the corporation acts on behalf of.

For trusts, a beneficial owner is defined as:

- An individual entitled to at least 25% of the trust property, whether vested or contingent.
- The settlor of the trust.
- A protector or enforcer of the trust.
- An individual with ultimate control over the trust.

KRYPTO BROKER INVEST must verify the information using reliable, independent documents or data, such as:

- Certificate of incorporation or registration
- Records from the relevant business registry
- Certificate of incumbency (if applicable)
- Constitutive documents (e.g., memorandum and articles of association, or partnership/trust deed)
    - For partnerships: confirmation of membership in a professional or trade association
    - For trusts: declaration of trust, deed of retirement and appointment of trustees, plus written confirmation from a professional trustee or lawyer
- Other relevant documents from independent sources (e.g., government-issued documents, independent registry reports, published or audited annual reports).

KRYPTO BROKER INVEST must take reasonable steps to verify client information, especially for companies with nominee shareholders or significant bearer shares. For clients with complex ownership structures, sufficient justification for the structure must be obtained.

The firm will audit transactions throughout the business relationship to ensure they align with client information and assess associated risks, including the source of funds. Regular reviews will keep client profiles updated, with high-risk clients reviewed every 6 months, medium-risk clients every 12 months, and low-risk clients every 24 months.

In trust scenarios, the trustee will be treated as the client. Their identity must be verified according to standard client identification requirements.

Documents must be dated within 3 months at the time of application. Acceptable proof of identity includes a clear ID document with a recent photograph, showing all borders, or a passport cover along with the personal information page.

We may be onboarding customers remotely, without physically witnessing the customer and his or her identity documents. Therefore, **KRYPTO BROKER INVEST** is required to have non-face-to-face verification measures in place, including but not limited to

- accepting only certified identification documents by lawyers or notaries public.
- holding a real-time video conference that is comparable to face-to-face. communication, in addition to providing electronic copies of identification. documents,
- verifying the identity of a customer through an official recognized authority (e.g... government),
- using new technology solutions including but not limited to biometric technologies (e.g., fingerprint, facial/voice recognition), which should be linked incontrovertibly to the customer.

For the purpose of (a), the certifier will need to have seen the original documentation. In. general, it is not sufficient for the copy documents to be self-certified by the client.

5. RISK ASSESSMENT

We shall adopt a risk-based approach in our KYC/AML process. Customer risk profiling evaluates risk factors based on individual circumstances, including significant aggravating and mitigating factors, to determine risk classification. This profiling occurs before establishing business relationships and periodically thereafter, or upon triggering events, to establish the necessary due diligence level.

Key risk assessment factors include:

- Country Risk
- Customer Risk
- High-Risk Industries and Businesses (Annex D)
- Ownership Risk (Annex E)
- Tax Risk
- Delivery/Distribution Channel Risk
- Product/Service Risk
  Each customer relationship will receive a risk classification based on this assessment, helping to identify potential misuse of our products for money laundering or terrorist financing.
  KRYPTO BROKER INVEST will periodically review existing relationships to detect any changes, analyze all transactions over the relationship, and identify any unusual or suspicious activity that may have been overlooked.

Customer Risk Level	Criteria	Review Frequency
Low risk	No risk criteria are fulfilled	2 Years
Medium risk	No risk criteria are fulfilled	1 Years
High risk	One or more risk criteria is identified	6 Months

- All documentation and supporting evidence of all risk profiling exercises conducted must be retained and recorded in adequate detail.

6. NAMES VERIFICATION

6.1. Overview

KRYPTO BROKER INVEST will screen all customers, authorized signatories, representatives, connected parties, and beneficial owners against relevant sanctions lists and sources related to money laundering and terrorism financing. This process identifies potential risks, connections to Politically Exposed Persons (PEPs), and any adverse news related to the customers.

The name screening ensures that all parties are checked against applicable sanctions lists for money laundering and terrorism financing risks. Positive matches must be escalated to the AML/CFT compliance function, with decisions documented at a senior level. A maker-checker process will be applied to all results, and potential matches will be thoroughly reviewed.

If a client or beneficial owner is identified as a PEP, approval from the MLRO and senior management is required before establishing a business relationship. If a screening indicates a terrorist association, we must block or freeze their assets and report the incident to local authorities.
We will also utilize public information to assess the reputation of customers and beneficial owners. Any allegations of wrongdoing will be analyzed for risk implications.

A database of terrorists and designated parties will be maintained to aid in identifying suspicious transactions. All search results and the rationale for dismissing positive matches must be documented. If a true positive match is confirmed, the account will not be opened, business relationships will be discontinued, and regulatory reporting will follow.

6.2. Sanctions lists original sources and Mandatory Sanctions List

The OFAC and UN Lists are global and not limited to specific regions or countries. When assessing name matches against international sanctions lists, the transaction must involve the country that issued the sanctions. For instance, if a transaction is from Germany to India and the recipient matches a name on the German list, it is a potential match. However, if the sender matches a name on the Panama list, it should not be considered a match.

Mandatory sanctions and screening lists are official documents maintained by governments and international organizations that identify individuals, entities, and countries subject to restrictive measures for reasons such as national security, human rights violations, or terrorism.

Krypto Broker Invest utilizes the following Mandatory Sanctions and Screening lists as part of its AML/CFT program:

- **Office of Foreign Assets Control (OFAC) List**: Maintained by the U.S. Department of the Treasury, this list includes Specially Designated Nationals (SDNs) and Blocked Persons.
- **United Nations Sanctions List**: Compiled by the UN Security Council, it includes individuals and entities under UN sanctions.
- **European Union Sanctions List**: Contains individuals and entities subject to restrictive measures by the EU.
- **UAE Cabinet Local List**: Includes individuals on the Local Terrorist List.

Screening must be conducted before executing any transaction.

6.3. Decision-making process

To verify if a customer matches a sanctions list, their ID (full name, date of birth, place of birth) must be compared with the list information. The more details available, the easier it is to determine if a match is true or false. Some lists offer minimal information, which may necessitate escalation to the MLRO.

The Compliance Officer or MLRO will follow these steps when checking customers against sanctions lists:

1. Evaluate potential name match.
2. Check date of birth
3. Check the place of birth.
4. Check country of residence
5. Check original source (e.g., OFAC, UN)
6. Check geographical matches.

If any criteria are met or there are questions about a match, it will be escalated to the MLRO.

All new customers are screened against government sanctions lists, and unresolved potential matches will be escalated to the MLRO. Existing customers will be periodically re-screened, with potential matches analyzed for accuracy.

After conducting Enhanced Due Diligence on a match, the MLRO will promptly report it to the UAE FIU and VARA.

7. TYPES OF HIGH-RISK CUSTOMERS

7.1. Politically Exposed Persons ("PEPs")

There are three types of PEPs:

- **Foreign PEP** - A foreign PEP is any individual who is or has been entrusted with a prominent public function in a foreign country and includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official but excludes a middle-ranking or more junior official, a spouse, a Partners, a child or a parent of a foreign PEP or foreign PEP's child, or a close associate of a foreign PEP,
- **Domestic PEP** - A domestic PEP includes all Government Ministers, Members of Parliament, Nominated Members of Parliament and Non-constituency Members of Parliament, their spouses, Partners or children, spouses, or Partners of their children, as well as close associates, and
- **International Organization PEP** - International organisations are entities established by formal political agreements between their member States that have the status of international treaties, their existence is recognised by law in their member countries, and they are not treated as resident institutional units of the countries in which they are located. Examples include the United Nations and affiliated agencies such as the International Maritime Organisation and International Monetary Fund, World Trade Organization, Asian Development Bank, Association of Southeast Asian Nations Secretariat, institutions of the European Union, Organisation for Security and Cooperation in Europe, military international organisations such as the North Atlantic Treaty Organisation, etc. Persons who have been entrusted with prominent functions by an international organisation are members of senior management such as directors, deputy directors and members of the board or equivalent functions.

These definitions help identify individuals with significant political influence.

7.2. Non-Governmental Organization and Charity Accounts

Unlike commercial and governmental sectors, NGOs (in many jurisdictions) often face minimal regulatory oversight. In many instances, the standards are very low, resulting in reduced scrutiny from authorities. This, coupled with a public presumption of honesty, weakens the external checks and balances essential for a healthy compliance environment, raising the risk of corruption and bribery.

8. SIMPLIFIED DUE DILIGENCE (SDD)

KRYPTO BROKER INVEST may conduct SDD to varying degrees if it determines that the risks of money laundering and terrorism financing are low. SDD will be performed only under specific circumstances and within the prescribed limits for each situation.

8.1. Dispensing with verification of beneficial owners

KRYPTO BROKER INVEST is not required to identify and verify the beneficial owners for certain types of clients or specific products related to client transactions. However, all other aspects of customer due diligence (CDD) must still be completed.

In general, simplified due diligence can be conducted to companies that belong to the categories described below,

- a regulated financial institution ("FI") that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.
- a corporation listed on the public stock exchanges in country that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; and
- an investment vehicle (e.g. a legal person/trust/collective investment scheme/other investment entity) where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is either:
    - a regulated or licensed fund manager in a country that is subjected to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

9. ENHANCED DUE DILIGENCE (EDD)

In the course of business, KRYPTO BROKER INVEST may identify a customer profile or transaction as high risk. Such cases must be escalated to the compliance department for evaluation. The MLRO will then determine if EDD is necessary and outline how it will be conducted. KRYPTO BROKER INVEST will perform enhanced due diligence for these customers, exceeding the standard CDD process.

9.1. EDD measures

Enhanced Due Diligence measures include, but are not limited to:

- Establishing, through appropriate means, the source of wealth and funds for the customer and any beneficial owners.
- Implement enhanced monitoring of business relations with the customer throughout the course of the relationship. KRYPTO BROKER INVEST will increase the intensity and nature of monitoring to identify any unusual or suspicious activities.
- Obtaining approval for Enhanced Due Diligence from the MLRO.

By conducting enhanced due diligence, we aim to gather additional information and evidence to better assess our customers' risk profiles and ensure compliance with our standards and risk appetite.

10. ONGOING MONITORING

KRYPTO BROKER INVEST will monitor customer profiles and transactions from the outset of the business relationship to ensure that activities align with the established risk profile. Periodic reviews will be conducted based on the frequency outlined in section 5, aimed at keeping all client information, data, and documents current. In addition to these periodic reviews, thematic or ad-hoc reviews may be initiated in response to external intelligence, news, or regulatory actions. Customer activities and profiles will be assessed, and Enhanced Due Diligence (EDD) may be implemented if connections to external triggers or suspicious transactions are identified. A suspicious transaction report may also need to be filed with VARA and relevant enforcement authorities.

Information about Virtual Asset transactions and VA Wallet addresses is inherently dynamic. Krypto Broker Invest will regularly evaluate and document the performance and effectiveness of any distributed ledger analytics tools used for ongoing monitoring.

11. FATF TRAVEL RULE

Before initiating any transfer of virtual assets valued over AED 3,500, KRYPTO BROKER INVEST must obtain and retain accurate originator and beneficiary information, making it available to VARA and relevant authorities upon request.

Similarly, beneficiary VASP must acquire and hold the required originator and beneficiary information before granting clients access to virtual assets from such transfers.

Required originator information includes:

- Name
- Account number or VA wallet address.
- Residential or business address

Required beneficiary information includes:

- Name
- Account number or VA wallet address.

Before engaging with a counterparty VASP or virtual asset service provider in another jurisdiction, KRYPTO BROKER INVEST must conduct risk-based due diligence to mitigate AML/CFT risks.

KRYPTO BROKER INVEST should adhere to the FATF Interpretive Note to Recommendation 15 and all applicable laws and regulations. It must also monitor any transactions attempting to circumvent regulatory thresholds related to the Travel Rule.

KRYPTO BROKER INVEST must, when applicable, establish internal controls to address the FATF Report on Virtual Assets Red Flags for Money Laundering and Terrorist Financing [September 2020] when developing transaction monitoring scenarios and thresholds to oversee clients' VA activities

12. TRANSACTION MONITORING

KRYPTO BROKER INVEST should monitor all transactions during business relations with customers, including one-off transactions. We manage tolerance levels, parameter settings, and sanctions lists, adjusting them based on emerging financial crime trends and transaction risks. Advanced blockchain analytics and AML tools help us identify abnormal customer behaviors.

If an irregular transaction is detected—such as high-risk activity that lacks a clear economic purpose or is inconsistent with the customer's background, an investigation process will be initiated. This may involve further inquiries, enhanced due diligence, and potential actions like account restrictions, risk-rating revisions, or regulatory suspicious transaction reporting (STR).

Transaction monitoring thresholds will be reviewed annually, aligning with industry standards and trends. A sandbox environment will be provided for the MLRO to test new risk rules against historical data, with results documented and communicated to the board, stored per the recordkeeping policy.

12.1. Transaction monitoring systems

- Actimize
- Chainalasys

12.2. Examples of suspicious transactions

FATF studies provide non-exhaustive examples of suspicious transactions. In assessing what constitutes suspicious, complex, unusually large, or abnormal transaction patterns, we take into account international typologies and insights from law enforcement and relevant authorities that may highlight jurisdiction-specific factors.

Common examples of suspicious transactions related to virtual assets include, but are not limited to:

- Transactions that cannot be reconciled with the customer's usual activities.
- A customer with multiple accounts or wallet addresses making frequent transfers between them.
- Withdrawals or transfers of virtual assets immediately after deposit, unless a plausible reason is provided.
- Unnecessary routing of funds to multiple intermediaries.
- Concentration of payments from multiple senders to a single account.
- Transactions with no clear relationship between the sender and beneficiary, or personal transfers to jurisdictions with no evident links to the customer.
- Large virtual asset deposits are inconsistent with the customer’s source of wealth or business activities.
- Frequent transfers to the same recipient.
- Rapid buying and selling of virtual assets over a short period.

- Multiple small transfers that collectively amount to a significant total.
- Ransom payments in virtual assets, such as Bitcoin, demanded through ransomware.

- Initial coin offerings or e-commerce scams involving virtual assets.
- Unauthorized transactions like hacking or theft of virtual assets.
- Use of mule accounts to exchange virtual assets through multiple hops in a short time.
- Transactions via decentralized exchanges or mixers.
- Opening mule accounts with stolen KYC information.
- Fund solicitation by terrorist groups or supporters using virtual assets.
- "U-turn" transactions, where funds received from a foreign source are transferred to another person or back to the sender.
- Sudden, frequent use of previously inactive accounts for large sums with no clear purpose.
- Transactions related to tax crimes.
- Rapid transfer of funds received from charitable organizations.
- Limited or no information on the origin of funds or virtual assets.
- Use of anonymization tools like VPNs or the Darknet to access accounts.
- Virtual-to-virtual layering schemes.
- Frequent changes in customer identification details.
- Requests for cash payments for the purchase or redemption of virtual assets.
- Reluctance to provide necessary identification or transaction details.
- Clients displaying nervousness or unusual behavior during transactions.
- Transfers to or from countries with high corruption, terrorism, or weak regulations.
- Transactions involving entities with no clear business purpose (e.g., shell companies).
- Mismatched or inconsistent client profile information.
- Funds from atypical sources for the client's profile.
- Altered documentation or mismatched client information.
- Transactions lacking a clear business rationale.

KRYPTO BROKER INVEST recognizes that blockchain technology can be vulnerable to criminal misuse because of its anonymity and capacity for efficient cross-border transactions. As a result, we maintain a list of prohibited uses of blockchain technology, where any indication of exposure will lead to account restrictions and Enhanced Due Diligence (EDD) measures.

12.3. Prohibited usage of blockchain technology

The list prohibited usage of blockchain technology is as follows:

- The usage of anonymity-enhanced features on the blockchain
    - Anonymity enhanced coins (also known as privacy features)
        - This includes any protocol that allows users to choose whether to activate anonymity features or not.
- Anonymity enhanced features that obfuscate the source of funds or trail of funds (e.g., mixers)

12.4 Risk Altering Procedures

Krypto Broker Invest has implemented alert thresholds and monitoring rules that initiate compliance reviews when VA transactions, wallet addresses, or client backgrounds indicate:

- A connection to criminal history or ongoing legal investigations.
- A match or potential match with sanctions lists.
- Involvement with privacy-enhanced coins or anonymizing protocols.
- Activity patterns that deviate from the customer's risk profile.

These alerts are promptly escalated to the Compliance and Operations teams, following established procedures for review, restriction imposition, and investigation.

13. SUSPICIOUS TRANSACTIONS REPORTING

If a staff member identifies any of the suspicious transactions listed, they must report it immediately to the MLRO and complete the Money Laundering Reporting Form (Annex A). The MLRO will acknowledge receipt of the report and remind the staff about their obligation to avoid tipping off.

Identifying suspicious transactions should lead to further inquiries about the transaction's purpose and beneficiary information, as well as investigations into the source of funds when necessary.

When evaluating the report, the MLRO should consider all relevant information, including Customer Due Diligence (CDD) and ongoing monitoring. This may involve:

- Reviewing transaction patterns and volumes across connected accounts.
- Referring to previous transaction patterns, the length of the business relationship, and CDD documentation.
- Questioning clients to identify other suspicious transactions as part of the Enhanced Due Diligence process.
-

If the MLRO deems it necessary to file a Suspicious Transaction Report (STR), it should be submitted promptly and reported to the board. Regular reports will also be sent to the UAE FIU and VARA via the GoAML platform. KRYPTO BROKER INVEST will continue monitoring transactions, filing additional STRs as needed.

The MLRO will maintain detailed logs of all escalated cases and report to the board on the measures taken. An STR register will document the outcomes of all investigations.

During regular monitoring, if there are grounds to suspect that a transaction's proceeds are related to a crime, the MLRO must:

- Report the suspicious transactions to the UAE FIU and VARA as per compliance rules.
- Respond promptly to requests for additional information from the UAE FIU and VARA within 48 hours.
- Undertake any required actions from the UAE FIU and VARA within specified timeframes.
- Inform the Compliance Officer (CO) about the STR if the MLRO and CO are different individuals, ensuring no tipping-off occurs.

The MLRO must take appropriate actions to mitigate the risk of KRYPTO BROKER INVEST being used for money laundering or terrorist financing, including strengthening AML/CFT processes and reviewing customer risk classifications. Any decision not to submit STRs for escalated suspicious transactions must be well-documented and substantiated.

14. RECORD KEEPING

KRYPTO BROKER INVEST must prepare, maintain, and retain records of all data, documents, and information required to meet AML/CFT obligations, in accordance with section H of the Compliance and Risk Management Rulebook from the Virtual Assets Regulatory Authority.

To meet these requirements, we will retain the following information:

- All Customer Due Diligence (CDD) information related to business relationships, value transfers, account files, and analysis results for at least eight (8) years after the termination of business relations or completion of transfers, or indefinitely for records related to UAE national security.
- All data and documents related to transactions, including explanations, for at least eight (8) years after the transaction's completion, or indefinitely for records related to UAE national security.
-

KRYPTO BROKER INVEST will keep:

- Original or copies of documents and records obtained during client identification and verification processes.
- Additional documents from the CDD and ongoing monitoring processes, including those for Simplified Due Diligence (SDD) and Enhanced Due Diligence (EDD).
- Documentation on the purpose and intended nature of the business relationship where applicable.
- Records related to the client's account, such as account opening forms, risk assessments, and relevant business correspondence.
- Details and results of any analyses conducted on complex, unusually large, or suspicious transactions.

15. BUSINESS AML RISK ASSESSMENT

KRYPTO BROKER INVEST periodically identifies and assesses the ML/TF risks we face to determine the necessary AML/CFT systems needed to mitigate those risks.

The Enterprise-wide Risk Assessment analyzes potential threats and vulnerabilities related to ML/TF exposure in our business. We assess the inherent ML/TF risks associated with our vendors and the effectiveness of our internal controls by following these steps:

- Evaluate the risks related to existing and new products/services, delivery channels, customer profiles, and countries associated with our vendors.
- Utilize relevant qualitative and quantitative data (such as the number of high-risk clients and compliance test results) to assist in the vulnerability analysis.
- Analyze the adequacy of current AML/CFT policies and procedures in addressing the identified risks.
- Develop an action plan to revise existing policies and procedures.
- Have senior management review, approve, and sign off on the Enterprise-wide Risk Assessment results and action plan.
- Implement the action plan effectively and provide sufficient internal guidance to staff.
- Maintain thorough records of all steps taken to enable regulators, auditors, and other stakeholders to conduct comprehensive review.

15.1. Methodology

KRYPTO BROKER INVEST adopts a straightforward conventional methodology of identifying and assessing the inherent risks present in each of the relevant risk factors/category, then will take into account the risk mitigating measures and controls in place to derive the overall residual risks.

15.2. Inherent Risks

Fundamentally, virtual assets (VA) present a high or even very high risk for money laundering, terrorism financing, and other financial crimes.

Inherent risk refers to the potential for ML/TF exposure without any control measures in place. Inherent risk ratings can vary based on the business' scope, size, and associated risks. The four recognized inherent risk factors in AML Risk Assessments for the financial services industry are: 1) customer, 2) products, services, transactions, and delivery channels, 3) geography, and 4) business strategy and regulatory environment.

Krypto Broker Invest assesses the business model and conduct of VA-related operations to identify unethical practices, governance issues, or market integrity concerns.

Additionally, Krypto Broker evaluates VA technologies—such as smart contracts, decentralized platforms, privacy coins, cross-chain protocols, and mixing services—for their potential to facilitate ML/TF activities during onboarding and ongoing compliance assessments

Each risk factor/category will be evaluated according to the level of inherent risks it poses, using the following scoring criteria:

Risk Score	Definition	Description
5	Very High	There is a very high level of ML/TF risks present in this risk factor/category.
4	High	There is a moderate to high (significant) level of ML/TF risks present in this risk factor/category.
3	Medium	There is a moderate level of ML/TF risks present in this risk factor/category.
2	Low	There is a low level of ML/TF risks present in this risk factor/category
1	Very Low	There is a low level of ML/TF risks present in this risk factor/category

15.3. Control Effectiveness

Mitigating controls encompass policies, procedures, organizational frameworks, programs, and other activities designed to protect the Company and counteract the inherent ML/TF risks associated with its operations.

Consequently, the effectiveness of the existing risk mitigating controls will be evaluated using the following scoring criteria to assess their strengths and weaknesses in adequately addressing the identified risks.

Risk Score	Definition	Description
1	Very Effective	• High level capabilities and control measures noted to address risks. • Implemented control measures are deemed highly effective. • Regular review and testing plans to evaluate effectiveness are in place for existing programs and control measures
2	Effective	• Medium to high level capabilities and mitigating control measures noted to address risks. • Implemented existing plans to achieve desired objectives and noted satisfactory results
3	Satisfactory	• Low to medium level capabilities and mitigating control measures noted to address risks. • Implemented some plans but with limited results noted in achieving desired objectives
4	Needs Improvement	• Some but not sufficient risk mitigating control measures to address risks. • Some but not sufficient immediate plans and actual actions taken to mitigate risks
5	Deficient	• Few or no mitigating controls to address risks. • No immediate plans and actual actions taken to mitigate risks

15.4. Quantitative and qualitative scoring

It is essential to conduct both a quantitative risk assessment, which relies on measurable and predefined data, and a qualitative risk assessment, which is based on the assessor's judgment and expertise (KRYPTO BROKER INVEST). Integrating these quantitative and qualitative assessments on an incremental scale is crucial to ensure that the evaluations are logical, robust, and mutually reinforcing.

Score	Inherent Risk Rating	Control Effectiveness Rating
$4.5 \leq x \leq 5$	Very High	Deficient
$3.5 \leq x < 4.5$	High	Needs Improvement
2.5 <= x < 3.5	Medium	Satisfactory
15 <= x < 2.5	Low	Effective
1 <= x < 1.5	Very Low	Very Effective

15.5. Deriving the residual risk

The calculation methodology outlined below is based on the principle that a robust control environment can reduce residual ML/TF risks relative to inherent risks.

The overall residual money laundering and terrorism financing risk to the Company is calculated as follows:

Inherent Risk Rating	Risk Mitigating Controls Strength	Overall Residual Risks
5- Very High	$1 \leq x < 1.5$	Medium
	1.5 ≤ x 2.5	High
	$2.5 \leq x < 3.5$	High
	$3.5 \leq x < 4.5$	Very High
	$4.5 \leq x \leq 5$	Very High
4-High	$1 \leq x < 1.5$	Medium
	$1.5 \leq x < 25$	Medium
	$2.5 \leq x < 3.5$	Medium
	$3.5 \leq x < 4.5$	High
	$4.5 \leq x \leq 5$	Very High
3- Medium	$1 \leq x < 1.5$	Medium
	$1.5 \leq x < 2.5$	Medium
	$2.5 \leq x < 1.5$	Medium
	$3.5 \leq x < 4.5$	High
	$4.5 \leq x \leq 5$	High
2- Low	$1 \leq x < 1.5$	Medium
	$1.5 \leq x < 2.5$	Medium
	$2.5 \leq x < 3.5$	Medium
	$3.5 \leq x < 3.5$	High
	$4.5 \leq x \leq 5$	High
1- Very Low	$1 \leq x < 1.5$	Medium
	$1.5 < x < 2.5$	Medium
	$2.5 < x < 3.5$	Medium
	$3.5 \leq x < 4.5$	High
	$4.5 \leq x \leq 5$	High

15.6. Control and Quality Assurance

Quality Assurance (QA) reviews are conducted periodically to ensure that decision-making remains accurate and consistent, and that AML risks are assessed appropriately and regularly.

The QA review process includes the following components:

- Periodic QA reviews involve sampling KYCs and transactions.
- QA reports are submitted to the MLRO regarding the KYCs and transactions reviewed.
- The MLRO evaluates the report.
- Any positive or negative findings from the MLRO's QA review will be documented. If negative results are identified, they will be communicated to management and addressed in periodic compliance meetings or other training sessions.

16. TRAINING AND EDUCATION

Training on anti-money laundering (AML) and anti-terrorist financing (CFT) will be provided to new staff during orientation to ensure they understand their obligations under relevant legislation.

Regular refresher training will reinforce staff responsibilities and update them on developments in AML/CFT, helping them recognize and report suspicious transactions.

The Compliance Officer will determine the frequency, content, and methods of ongoing training based on business needs. Training will cover AML/CFT laws, emerging trends, and updates to internal policies. Training effectiveness will be monitored through tests, compliance checks, attendance tracking, and follow-ups with staff who miss training sessions.

KRYPTO BROKER INVEST will maintain records of training participants, dates, and content for a minimum of 8 years.

17. FORMS

All staff and licensed individuals must complete a Staff AML/CFT Acknowledgement Form (Annex C) upon joining the Company and at least annually thereafter.

18. ANNUAL AUDIT

KRYPTO BROKER INVEST will conduct periodic audits of our AML/CFT framework, including sample testing, to evaluate the effectiveness of measures against money laundering and terrorism financing. These

audits will assess the adequacy of our AML/CFT policies, procedures, controls, risk assessment framework, and the application of a risk-based approach. They will also review the content and frequency of AML/CFT

training programs and employee compliance with this Manual, as well as the timely reporting of non-compliance to senior management.

The audits will include a review of whether the technology used for non-face-to-face verification is as robust as face-to-face methods. An independent assessment by a qualified professional will be required to certify the effectiveness of any new technology in managing impersonation risk, both at the one-year mark after implementation and on an ongoing basis.

The first audit must be completed promptly after starting digital operations, with the report submitted to VARA within one year. Subsequent audits will occur annually or after significant changes to AML/CFT policies, whichever comes first.

An independent external auditor will conduct a third-party attestation of this Policy, reviewing its implementation and effectiveness. The attestation report will be submitted to VARA annually or upon request.

Annex A Money Laundering Reporting Form

KRYPTO BROKER INVEST

Anti-Money Laundering and Counter-Financing of Terrorism Policy and Procedures

Name of reporting staff:

Department:

Name of suspicious client:

Date of contact with client:

Nature of business:

*Optional

Details of the transaction causing suspicion and any other relevant information:

Noted by the Compliance Officer:

Signature

Date:

Annex B Suspicious Transaction Report

KRYPTO BROKER INVEST

Anti-Money Laundering and Counter-Financing of Terrorism Policy and Procedures

A Suspicious Transaction Report (STR) should include the following details:

- personal particulars (name, identity card or passport number, date of birth, address, telephone number, bank account number) of the person(s) or company involved in the suspicious transaction,
- details of the suspicious financial activity,
- The reason the transaction is suspicious: which suspicious activity indicators are present?
- the explanation, if any, given by the person about the transaction

The laws state that when a person knows or suspects that any property is proceeds of drug trafficking or an indictable offence, or terrorist property, or was used in connection with drug trafficking, an indictable offence or terrorist act, or is intended to be used in drug trafficking. an indictable offence or terrorist act, he or she should report his or her knowledge or suspicion to an authorised officer as soon as practicable.

Submit a STR by email to [email address of CBUAE FIU or via GoAML portal.

Annex C Staff AML/CFT Acknowledgement Form

KRYPTO BROKER INVEST

Anti-Money Laundering and Counter-Financing of Terrorism Policy and Procedures

I hereby acknowledge that I have read and understand the Anti-Money Laundering and Counter-Financing of Terrorism Policy and Procedures (the "AML/CFT Policy") of **KRYPTO BROKER INVEST**. I agree that I will comply with the AML/CFT Policy and will cooperate with any investigations or inquiries to determine whether any violations of the AML/CFT Policy have occurred.

I understand that I am responsible for reporting any suspicious activity to the MLRO and any failure to comply in all respects with the foregoing or the AML/CFT Policy may lead to internal penalties up to and including dismissal, and to significant external criminal, civil and disciplinary penalties.

Signature

Name

Date

Annex D High Risk Industries and Businesses

KRYPTO BROKER INVEST

Anti-Money Laundering and Counter-Financing of Terrorism Policy and Procedures

We have identified certain Industries/ Businesses as being more susceptible to money laundering than others. Customers who are involved in the following industries and businesses may pose a higher ML/TF risk.

1. Armament or Weapons Related Industries

This category includes manufacturers, dealers and intermediaries of explosives or armament and strategic goods. Strategic goods are military goods or goods capable of military uses include nuclear biological and chemical weapons, conventional arms, and dual-use items, which can be used for both civilian and military applications.

To manage the risk of proliferation financing via products and services, special attention should be given to customers whose business activities involve dual-use goods, especially nuclear-related items, and technologies.

Customers in the armament or weapons related industries are rated automatically High Risk

2. Casinos, Junkets, Betting and Other Gambling Related Businesses

This industry may present a higher risk of money laundering because, among other reasons:

- In some countries, such businesses are delivered to be closely associated with organised crime.
- Such businesses operate in a cash-intensive environment, providing higher opportunities for both operators and customers to launder funds.
- In some counties, such businesses operate with little or no regulatory, or government oversight.

The potential ML/TF risk is even greater for internet-based gambling enterprises where there is no face-to-face contact with gambling customers.

Enhanced due diligence measures need to be applied to verify business activities, and the adequacy of the ML/TF risk control measures implemented to assess the potential risk involved in dealing with such customers.

Customers that are casinos, junkets, betting, or other gambling related businesses are rated automatically High Risk.

3. Money Services Businesses ("MSBs").

MSBs provide an attractive alternative for money launderers as compared to banks, which are more closely regulated and supervised. Examples of such businesses would include remittance houses, currency exchange houses, casas de cambio, bureau de change, money transfer agents and bank note traders or other businesses offering money transfer facilities.

Money changers and remittance agents collectively known as MSB are rated automatically at High Risk

4. Precious metals, stones, and high-end luxury goods

Dealers in high value or precious goods are given higher opportunities for abuse by money launderers. Money launderers attempt to move illicit funds undetected through transacting with these dealers and disguise criminal proceeds as legitimate transactions.

Natural persons or legal entities associated with precious metals, precious stones mining operations including its intermediate brokers or buyers, Antiques, art Works, Jewelry, Diamond, and scrap markets are rated automatically High Risk.

5. Charitable and Other Non-Profit Organisations/Foundations ("NPOS")

Charities and other non-profit organisations are at risk of being misused for illicit purposes. They are susceptible to criminal abuse by money launderers or deviant organisations due to the following reasons.

- They may pose as legitimate entities to Conduct criminal activities.
- They may be exploited by or actively supported by terrorists or terrorist organisations to escape asset freezing measures.
- They may be used to conceal or obscure the clandestine diversion of funds intended for legitimate purposes but diverted for terrorist purposes.

Our entities are to understand the purpose and management of the administration of the Charities and other non-profit organisations. In addition, our entities should ascertain if NPOS are subjected to supervision and regulation by authorities for governance and financial controls.

6. Embassies and Foreign Consulates

Embassies and foreign consulates are at risk of money laundering because they can abuse their diplomatic access to laundering money for corrupt politicians, their family members, or close associates.

For example, accounts of embassies or foreign consulates may pose a higher risk. In the following circumstances.

- Accounts are from countries that have been designated as higher ML/TF risk. Substantial cash transactions take place in the accounts.
- Account activity is not consistent with the purpose of the account.
- Accounts that directly fund personal expenses for foreign nationals, including but not limited to expenses for college students,
- Official embassy business Is conducted through personal accounts of members of the diplomatic staff.

In carrying out the customer due diligence, we should establish the purpose of the business relations and should be vigilant for accounting activities which are not commensurate with official embassy business.

7. Entertainment

Natural persons or legal entities associated with entertainment activities (e.g., Betting activities Night Clubs, Karaoke Discotheques, Amusement game centers, other miscellaneous entertainment activities.)

8. Financial Entities without License

Natural persons or legal entities may provide financial services to their customers without proper license, KYC and AML. controls may be insufficient and therefore, likely to attract and interact with illicit funds in the market. Therefore, companies that engage in financial activities without license or regulations are rated automatically High-Risk. This also includes unregulated VASPs due to regulatory sunrise issues.

Annex E Ownership Risk

KRYPTO BROKER INVEST

Anti-Money Laundering and Counter-Financing of Terrorism Policy and Procedures

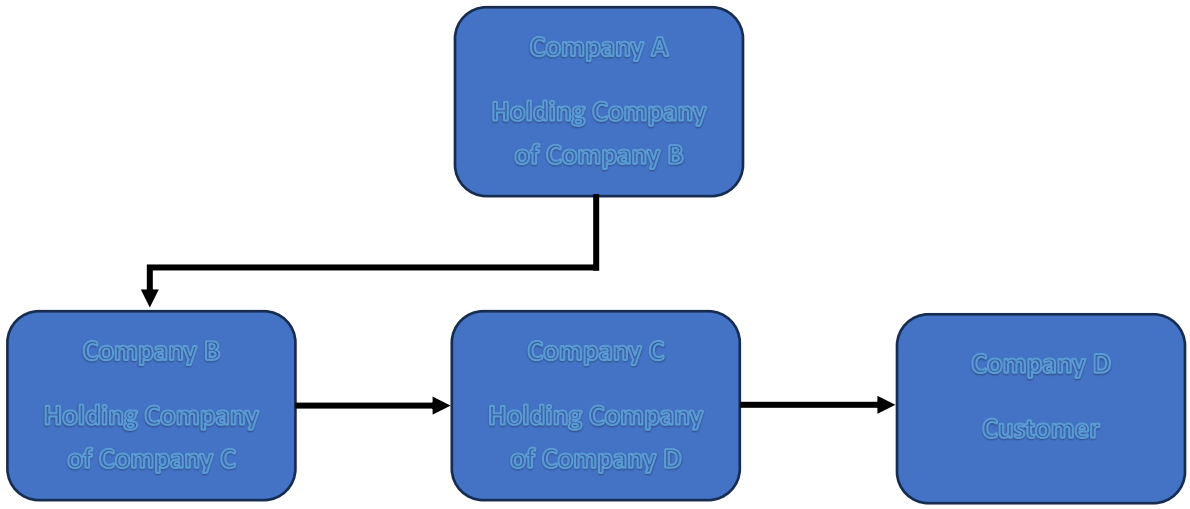
Methodology applied to determine the risk of Ownership Risk

Upon the relevant business Is identified for the customers, the ownership risk shall be considered as according to the following methodology.

No.	Risk Factors	Risk Level
1	For personal accounts: use of non-spouse POA	High
2	For entity accounts: entities with complex structure involved (refer to below Complex Structure)	High

Complex Structure refers to a corporate or legal entity involving three layers or more in the Ownership chain as illustrated as below:

DIAGRAM



www.kryptobrokerinvest.ae
va@kryptobrokerinvest.ae
Office # M2-136 , Building BN COMPLEX, Al Muteena , Dubai , UAE.
+971 50 294 3100