حكومة دبي
GOVERNMENT OF DUBAI

سُلطة تنظيم الأصول الافتراضية
VIRTUAL ASSETS REGULATORY AUTHORITY

Compliance and Risk Management Rulebook

7 February 2023

varaconnect@vara.aeصندوق بريد: 9292 دبي، الإمارات العربية المتحدة - سُلطة تنظيم الأصول الافتراضية
varaconnect@vara.ae - PO Box 9292, Dubai, UAE - Virtual Assets Regulatory Authority

Contents

Introduction

The Dubai Virtual Assets Regulatory Authority [**VARA**] was established and authorised by *Law No. [4] of 2022 Regulating Virtual Assets in the Emirate of Dubai* [**Dubai VA Law**] to regulate Virtual Asset Service Providers [**VASPs**].

This Compliance and Risk Management Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023 [the **Regulations**] issued by VARA and applies to all VASPs Licensed by VARA to carry out any VA Activity in the Emirate.

This Compliance and Risk Management Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out any VA Activity must also comply with the following Rulebooks applicable to all VASPs:

- Company Rulebook;
- Technology and Information Rulebook;
- Market Conduct Rulebook; and
- All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

Capitalised terms in this Compliance and Risk Management Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 1.

Unless otherwise stated, all requirements in this Compliance and Risk Management Rulebook are Rules and have binding effect.

Part I – Compliance Management

Introduction

Part I of this Compliance and Risk Management Rulebook sets out:

- General principles for regulatory compliance;
- The implementation of a compliance management system including appointing a Compliance Officer [**CO**];
- Management, operations and information risk;
- Record keeping and audit; and
- Employee management and training.

A. General principles

VASPs shall comply with the spirit of the following principles when conducting all their business from or through, or servicing the Emirate, including all VA Activities.

1. *Integrity – honesty and fairness*: VASPs should act truthfully, justly and equitably, in good faith serving the best interests of their clients, yet at all times preserving market integrity.
2. *Diligence*: VASPs should act with due skill, care and diligence reasonably expected of a VASP of a similar nature and/or catering to a similar activity.
3. *Capabilities*: VASPs should have, and effectively employ necessary resources [financial, technical or otherwise] and procedures for the sound, effective and efficient operation of their business, including VA Activities.
4. *Client assets*: VASPs should ensure that client assets are promptly and properly accounted for, and adequately safeguarded.
5. *Effective disclosures*: VASPs should ensure that any disclosure is clear, concise and effective, and contains information necessary for their clients to make an informed decision and be kept up-to-date. VASPs should dispatch information in a timely manner if ongoing disclosure is required by relevant authorities, including VARA, or under any fiduciary duty owed by VASPs to their clients.
6. *Compliance*: VASPs should devise effective strategies to ensure ongoing compliance with—
   a. all legal and regulatory requirements [including any conditions in respect of a Licence] applicable to the conduct of their business, including VA Activities; and

b. their own constitutional documents, internal policies and controls,

so as to promote the best interests of their clients and for promoting the integrity of the market.

7. *Dealings with regulators.* VASPs should act in an open and transparent manner with regulators at all times, including VARA.

B. Compliance management system

1. VASPs shall establish and maintain an effective compliance management system [**CMS**] which—

   a. covers all relevant aspects of their operations, including the unfettered access to necessary records and documentation by the Board and relevant Staff;

   b. is independent of all operational and business functions;

   c. ensures that the CO is notified of any material non-compliance promptly;

   d. comprises technical competence, resources [including financial and non-financial] and experience necessary for the performance of their functions; and

   e. comprises a testing and monitoring programme that is risk-based and designed to regularly select and review different areas of the business and analyse key performance and risk indicators,

   in order to allow them to identify potential compliance violations and to ensure that they comply with all applicable laws and regulatory requirements, and their own internal policies and procedures at all times.

2. The CO shall ultimately be responsible for establishing and administering the CMS and notifying VARA and other relevant authorities of the occurrence of any material non-compliance by the VASP, its Board or its Staff with applicable legal and regulatory requirements.

3. VASPs shall establish, maintain and enforce clear and detailed compliance policies and procedures to enable all Staff and the Board to—

   a. comply with all applicable legal and regulatory requirements at all times, including all conditions in respect of a Licence, record keeping, business practices, AML/CFT, and compliance with relevant client, proprietary and Staff dealing requirements;

   b. ensure that client complaints are handled properly with appropriate remedial action. Complaints should be handled and investigated by Staff who are not directly involved in the subject matter of the complaint; and

c. have access to all necessary information required to perform a business transaction.

4. The CMS and the compliance policies and procedures shall be reviewed and updated from time to time to ensure that they are aligned with the changing business and regulatory landscape applicable to the global Virtual Asset sector.

5. VASPs shall ensure that all Staff performing compliance functions are Fit and Proper Persons and possess the necessary skills, qualifications and experience for their roles.

6. To the extent that VASPs carry out any VA Activities or similar business activities anywhere other than the Emirate, VASPs shall comply with all applicable law and regulatory requirements in any jurisdiction in which they carry out such VA Activities or similar business activities.

C. Duties of the Compliance Officer

1. VASPs shall appoint a CO who—

a. possesses at least five [5] years of relevant experience in a compliance function;

b. is a Fit and Proper Person as approved by VARA;

c. is a resident in the UAE or holds a UAE passport;

d. is a full-time employee of the VASP; and

e. reports directly to the Board.

Such appointment shall be reviewed annually to ensure that the CO remains a Fit and Proper Person capable of discharging all relevant duties. VARA has the sole discretion to request a VASP to provide such evidence as VARA may require which shows that the above requirements are satisfied.

2. The CO shall be responsible for—

a. ensuring Staff, including Senior Management, are properly and adequately trained in respect of their understanding and compliance with all applicable laws and regulatory requirements, including those relating to consumer protection and AML/CFT;

b. developing and implementing compliance policies and procedures, including a Business Continuity and Disaster Recovery Plan [**BCDR Plan**] as required in the Technology and Information Rulebook;

c. assessing emerging issues and risks;

d. reporting compliance activities and compliance audits to the Board; and

e. if necessary, ensuring appropriate corrective actions are taken in response to deficiencies in the CMS and/or non-compliance with any applicable laws or regulatory requirements.

3. Compliance activities may be delegated to appropriate professionals, provided that—

a. the CO shall continue to be held accountable for all responsibilities and obligations in relation to the implementation of the CMS; and

b. all applicable requirements in the Company Rulebook, including Outsourcing management requirements, are complied with.

4. Subject to relevant requirements in the Company Rulebook and if deemed appropriate by the VASP, the CO may hold more than one [1] non-client facing role within the VASP, provided such roles do not create conflicting duties, including but not limited to, the Money Laundering Reporting Officer [**MLRO**] and the head of the risk function. VARA will take into account other roles held by the CO in determining whether the individual is a Fit and Proper Person.

D. Risk management

1. VASPs shall establish and maintain—

a. an effective risk management function;

b. policies and procedures; and

c. risk measurement and reporting methodologies,

commensurate with the nature, size, complexity, and risk profile of the VASP in order to identify, measure, quantify, manage and monitor the risks, whether financial, technological or otherwise, to which they are or may be exposed. Such policies and procedures should be followed strictly to ensure that risks are maintained at acceptable and appropriate levels.

2. The risk management function should consist of a sufficient number of suitably qualified and experienced Staff. The head of the risk function of a VASP must have the appropriate qualifications and authority to oversee and monitor the overall risk exposures of the VASP. The CO may also be the head of the risk function. If the head of the risk function is a separate individual from the CO, the head of the risk function must also report directly to the Board of the VASP.

3. The Board shall ensure that the risk management policies are subject to ongoing comprehensive review, particularly when there is a material change in the VASP's business, operations or Senior Management or Staff, or to the market conditions and applicable laws and regulations that may affect the risk exposure of the VASP.

4. The head of the risk function of a VASP shall submit risk exposure reports to the Board which identifying and report all actual or potential risks. Such reports must be submitted to the Board at least once every quarter, or more frequently if required for the VASP to address a specific risk which been identified.

5. The effectiveness of the risk management policy of each VASP will depend on the types of risks associated with the VASP and its business operations, including the VA Activities it carries out. The key types of risks that must be considered by all VASPs, and reported in the risk exposure reports under Rule I.D.4 of this Compliance and Risk Management Rulebook above to the extent they are applicable, and the mitigating measures which must be adopted for each type of risk include, but are not limited to—

    a. Financial stability risks.

        i. *Financial soundness*: Risks arising when a VASP lacks the necessary capital, liquidity or reserves to run operations [both in the going-concern and wind-down scenario] and meet all commitments to its clients, including but not limited to when a VASP is likely to be unable to comply with any of its Capital and Prudential Requirements in the Company Rulebook.

        ii. *Market risk*: Risks arising from the type and nature of market risk undertaken by the VASP [e.g. the nature of market risk exposure of the VASP's services and VA Activities]. In relation to such risks, VASPs shall adopt mitigating measures including but not limited to—

            1. regular control techniques to monitor market risks, including conducting regular reviews of financial statements and the value of their Virtual Asset holdings; and

2. establish and maintain effective risk management measures to quantify the impact of changing market conditions on themselves and their clients. Factors to be considered include—

   (a) unspecified adverse market movements [including but not limited to "flash crashes", catastrophic risk or tail events], by using an appropriate value-at-risk model or other methodology to estimate potential loss;

   (b) individual market factors, to measure the sensitivity of the VASP's risk exposure to specific market risk factors; and

   (c) stress testing, determining the effect of material changes in market conditions [whether or not specific to Virtual Asset markets] on the VASP using quantitative and qualitative variable assumptions.

iii. *Credit risks*: Risks arising from the type and nature of credit risk undertaken by the VASP [e.g. the nature and level of credit risk exposure of the VASP's services and VA Activities]. In relation to such risks, VASPs shall adopt mitigating measures, at both an individual account and consolidated account level, including but not limited to—

1. establish and maintain an effective credit rating system to evaluate the creditworthiness of their clients and counterparties;
2. adopt clearly defined objective measures to evaluate potential clients and counterparties and to determine or review the relevant credit ratings which are used to set appropriate credit, trading and position limits for all clients and counterparties, which shall be enforced at all times;
3. use appropriate quantitative risk measurement methodologies to effectively calculate and monitor the credit exposure of VASP in relation to clients and counterparties, including pre-settlement credit exposures and settlement risks. Credit risks posed by all clients and counterparties

belonging to the same group of Entities can be aggregated for the purpose of measuring the credit exposure of the VASP;

4. if applicable in respect of the VA Activities of the VASP, establish and maintain all policies in respect of margin required under any Rulebook, which notwithstanding all other requirements in those Rulebooks should include—

   (a) the types of margin which may be called, the applicable margin rates and the method of calculating the margin;

   (b) the acceptable methods of margin payment and forms of collateral;

   (c) the circumstances under which a client or counterparty may be required to provide margin and additional margin, and the consequences of a failure to meet a margin call, including the actions which the VASP may be entitled to take; and

   (d) applicable escalation procedures where a client or counterparty fails to meet successive margin calls.

iv. *Liquidity risks*: Risks arising from the type and nature of the VASP's liquidity or asset and liability mix. In relation to such risks, VASPs shall adopt mitigating measures including but not limited to—

1. enforce concentration limits with respect to particular products, markets and counterparties, taking into account their liquidity profile and the liquidity profile of the VASP;
2. regularly monitor any maturity mismatch between sources and funding requirements and concentrations of individual Virtual Assets, markets and counterparties; and
3. establish clear default procedures to alert relevant Staff and Senior Management to potential liquidity problems and to provide such Staff and Senior Management with sufficient time to minimise the impact brought by any client's or counterparty's liquidity issues.

b. Market conduct risks.

i. *Business strategy*: Risks arising from the overall strategy and current sources of business of the VASP [e.g. strategic planning process and achievability of strategy].

ii. *Client onboarding risks*: Risks arising from onboarding clients [individuals and corporates]. This refers to the level of client due diligence [**CDD**] applied, such as sanction screening, risk rating and watchlist screening.

iii. *Organisation and regulation*: Risks arising from the structure of a VASP, the characteristics and nature of responsibilities of UBOs, Board members and Senior Management responsibilities.

iv. *Operational risks*: Risks arising from type and nature of operational risk involved in the VASP's activities [e.g. direct or indirect loss from inadequate or failed internal processes, systems or external events].

v. *Quality of management & corporate governance*: Risks arising from the quality of the VASP's management, the nature of the corporate governance, management information and compliance culture, including but not limited to non-compliance with relevant requirements in the Company Rulebook.

vi. *Relationship with regulators*: Risk arising from the nature of the VASP's relationship with other regulators, including recent regulatory history.

vii. *Cybersecurity risks*: Risks of exposure or loss from a cyber-attack, data, system or security breach, including any breach of Personal Data security, not limited to non-compliance with relevant requirements in the Technology and Information Rulebook. VASPs must also include all risks relating or the VASP's reputation in such events.

c. Compliance and risk management risks.

i. *AML/CFT, market abuse & fraud*: Risks arising from the VASP's susceptibility to financial crime risk arising from money laundering, market abuse, terrorism financing, and fraud, including but not limited to non-compliance with relevant requirements in this Compliance and Risk Management Rulebook.

ii. *Outsourcing & counterparty risks*: Risks arising from Outsourcing to third parties, developing relationships or dependencies on counterparties in any transactions, including with any Controlling Entity, Group Entity or UBO.

iii. *Risk management systems*: Risks arising from the nature and effectiveness of the systems and procedures to identify, measure, monitor and control the VASP's risks [e.g. credit risk, insurance underwriting risk, market risk, operational risk, legal risk and new product risk].

iv. *Compliance function and arrangements*: Risks arising from the nature and effectiveness of the compliance function of a VASP. These include its mandate, structure, staffing, methodology, reporting lines and effectiveness.

v. *Business continuity*: risks arising from the effectiveness of business continuity arrangements, including but not limited to non-compliance with relevant requirements in this Compliance and Risk Management Rulebook.

d. Consumer protection risks.

i. *Communications with clients & financial promotions*: Risks arising from the nature of financial promotion and advertising practices employed by the VASP, including but not limited to non-compliance with relevant requirements in the Market Conduct Rulebook.

ii. *Legal risks*: Risks arising from the nature of the VASP's contractual agreements.

iii. *Disclosure and reporting*: Risks arising from the nature of terms of business, periodic statements and other documentation provided to clients, including but not limited to non-compliance with relevant requirements in the Market Conduct Rulebook.

iv. *Client assets*: Risk arising from the VASP holding or controlling of Client Money and Client VAs.

E. Operation management

1. VASPs shall establish and maintain effective operational policies and processes to ensure—

a. they have regular exchange of information with their clients, Group and, where appropriate, counterparties;

b. the integrity of their dealing practices, including the treatment of all clients in a fair, honest and professional manner;

c. the safeguarding of both their assets and all Virtual Assets [including Client VAs] in accordance with applicable requirements in this Compliance and Risk Management Rulebook and the Technology and Information Rulebook;

d. the maintenance of proper records and the reliability of the information contained in such records in accordance with applicable requirements in this Compliance and Risk Management Rulebook; and

e. the compliance by VASP and all its Staff with all applicable laws and regulatory requirements.

2. Where a VASP may act on behalf of the client in relation to the operation of an account, it shall properly communicate to the client the necessary procedures and terms and conditions under which the VASP may act on its behalf in transactions which are consistent with the stated objectives of the client and strictly follow such procedures.

3. In addition to applicable requirements in the Market Conduct Rulebook, VASPs shall establish and enforce procedures to ensure that there are safeguards against any of their Staff or members of the Board taking advantage of confidential information or Inside Information.

4. In addition to applicable requirements in the Technology and Information Rulebook, VASPs shall establish and maintain robust procedures to protect their Virtual Assets and Client VAs from theft, fraud and/or misappropriation. All Staff and members of the Board should follow all applicable internal protocols to acquire, transfer or otherwise dispose of any of the VASP's Virtual Assets and Client VAs in accordance with applicable requirements in this Compliance and Risk Management Rulebook and the Technology and Information Rulebook.

5. VASPs shall regularly check all—

a. records and reports, whether issued by third parties, such as banks, other VASPs, or other virtual asset service providers outside of the Emirate; and

b. relevant information recorded on all systems including distributed ledgers,

and reconcile the above with their internal records for the purpose of identifying any errors, omissions or misplacement of assets, including Virtual Assets.

6. VASPs may establish committees as they deem appropriate in order to ensure compliance with all applicable laws and regulatory requirements. VARA may require a VASP, either as a condition of granting a Licence or at any stage thereafter, to establish any committee[s] determined by VARA as it deems appropriate, and VASPs shall comply with such requirements.

F. Books and records

1. VASPs shall keep their books and records properly in their original form or native file format [including as recorded on distributed ledgers where appropriate], including—
   a. keeping proper audit trails of all transactions, such as the amount, date and time of each transaction, any payment instruction, the total amount of fees and charges, the names, details of accounts or VA Wallets and country of residence of the clients and to the extent practicable, that of any other Entities involved in the transaction, so as to enable the VASP to carry out thorough investigation of any Suspicious Transactions [subject to further requirements set out in Part III of this Compliance and Risk Management Rulebook];
   b. maintaining and organising all information relating to clients produced by third parties;
   c. maintaining sufficient records to prove that the VASP is in compliance with all applicable laws and regulatory requirements, including AML/CFT laws and requirements in Part III of this Compliance and Risk Management Rulebook;
   d. keeping proper records to enable the VASP to carry out an audit in a convenient manner;
   e. keeping a general ledger containing all assets [including Virtual Assets], liabilities, ownership equity, income and expense accounts;
   f. keeping statements or valuations sent or provided to clients and counterparties;
   g. keeping minutes of meetings of the Board;
   h. retaining communications and documentation related to investigations of client complaints and transaction error resolution or concerning facts giving rise to potential violation of laws and regulatory requirements; and
   i. maintaining a conflicts of interest register in accordance with the Company Rulebook.

2. VASPs shall retain each such record as set out in Rule I.F.1 of this Compliance and Risk Management Rulebook in accordance with the following timelines—
   a. no less than eight [8] years; or
   b. for an indefinite period for all records which may relate to national security of the UAE.
3. VASPs shall furnish copies of any records to VARA in accordance with all applicable requirements in the Regulations, Rules or Directives.

G. Audit

1. External audit.
   a. VASPs shall appoint an independent third-party auditor to perform an audit of the financial statements of the VASP in order to make available an annual report, and promptly notify VARA of the full name and contact details of the auditor upon appointment.
   b. The annual report of VASPs shall promptly be made available to their clients and VARA upon request.
   c. VASPs should understand the steps taken by the auditor in proving the existence and ownership of Virtual Assets and ascertaining the reasonableness of the valuation of Virtual Assets.
   d. The accounting information given in the annual report shall be prepared in accordance with generally accepted accounting principles.
   e. If requested, VASPs shall procure relevant counterparties to cooperate with the auditor and to provide with the auditor all necessary information for the auditor to conduct the audit.
   f. VARA may in its sole and absolute discretion require a VASP to appoint alternative auditors if their original auditors are not deemed appropriate for the size and complexity of their business and in terms of reputation.
2. Internal audit.
   a. VASPs shall, where applicable, establish and maintain an objective internal audit function which shall be independent of the operational function and submit regular reports directly to the Senior Management.

b. VASPs shall establish and maintain clear policies in defining the role and responsibilities of, and the working relationship between, the internal and external auditors.

c. The internal audit function shall—

i. perform audit work regularly and at least on a quarterly basis;

ii. inform the Senior Management of findings and recommendations; and

iii. follow up with and resolve matters or risks highlighted in the relevant reports.

H. Regulatory reporting

1. On a monthly basis, VASPs shall as a minimum submit to VARA the following information—

a. their balance sheet and a list of all off-balance sheet items;

b. their statement of profit and loss;

c. their income statement;

d. their cashflow statements;

e. addresses of their VA Wallets;

f. a full list of Entities in their Group that actively invest their own, or the Group's, portfolio in Virtual Assets, and a complete record of all transactions, including but not limited to loans or any transactions involving any VA Activity for which the VASP is Licensed, with all such Entities identified; and

g. transactions with Related Parties as prescribed in the Company Rulebook.

2. On a quarterly basis, VASPs shall as a minimum submit to VARA the following information—

a. the minutes of all Board meetings and Board committee meetings;

b. a statement demonstrating compliance with any financial requirements established by VARA including but not limited to Reserve Assets;

c. financial projections and strategic business plans; and

d. a risk exposure report prepared and submitted to the Board in accordance with Rule I.D.4 of this Compliance and Risk Management Rulebook.

3. On an annual basis, VASPs shall as a minimum submit to VARA the following information—

a. audited annual financial statements, together with an opinion and an attestation by an independent third-party auditor regarding the effectiveness of the VASP's internal control structure;

b. an assessment by Senior Management of the VASP's compliance with such applicable laws, Regulations, Rules and Directives during the fiscal year covered by the financial statements;

c. certification of the financial statements by a member of the Board or a Responsible Individual attesting to the truth and correctness of those statements;

d. a representative sample of all documentation relating to client onboarding [including actual documentation of the first one hundred [100] clients onboarded of the year];

e. descriptions of product offerings relating to their VA Activities;

f. Group structure chart including shareholding of the VASP and the identity of all UBOs;

g. the names of each of the members of the Board and the Senior Management in the VASP, a brief biography of each such member including their qualifications and experience and any position that a member of the Board or the Senior Management holds in other Entities;

h. the identification of any independent director[s] if applicable;

i. the names of all the members of any committees, the authorities and assignments entrusted thereto, and activities carried out by the committees during that year; and

j. the number of meetings held by the Board and the committees, and the names of the attendees.

4. VARA may require upon request to a VASP, information to be provided in addition to those listed in Rule I.F.1 of this Compliance and Risk Management Rulebook.

I. Regulatory notifications

1. VASPs shall notify VARA in writing of—

a. any changes to items set out in Rule I.H.3 of this Compliance and Risk Management Rulebook; and

b. any criminal or material civil action, charge or proceedings or Insolvency Proceedings, or any investigations, inspection or enquiries which may lead to any such action, charge or proceedings, made against the VASP or any of its Board members, UBOs or Senior Management immediately after the commencement of any such action, charge, proceeding, investigation, inspection or enquiry.

2. VASPs shall submit a report to VARA immediately upon the discovery of any violation or breach of any law, Regulation, Rule or Directive related to the conduct of any VA Activity.
3. VASPs shall, upon request from VARA, disclose information regarding their activities in jurisdictions other than the Emirate.
4. VASPs shall comply with all requirements in the Technology and Information Rulebook with regards to notifying VARA of incidents relating to a cybersecurity breach, including but not limited to incidents involving a loss of information or affecting Personal Data.

J. Staff management and training

1. VASPs shall implement procedures to ensure that they only employ suitably qualified individuals with the requisite skills, knowledge and expertise to perform the duties for which they are employed and that such individuals are duly registered with all applicable professional bodies as required.
2. VASPs shall employ appropriate numbers of Staff to discharge relevant duties effectively. Unless otherwise stated in the Regulations and Rulebooks, Staff are not required to be physically located in the Emirate, provided that the VASP is able to ensure that all supervisory, monitoring and enforcement functions are effectively implemented to VARA's satisfaction.
3. VASPs shall ensure that all Staff are provided with adequate and up-to-date information regarding all their policies and procedures.
4. Adequate training suitable for the duties which the Staff is required to perform in their role shall be provided at the beginning of their employment and on an ongoing basis.
5. VASPs shall implement and provide AML/CFT training for all Staff on a regular basis and monitor their compliance with all established procedures.
6. VASPs shall make necessary arrangements to ensure that all operational policies and procedures are communicated to new hires within their first thirty [30] calendar days of starting their employment.
7. In the event that the operational policies and procedures are updated, VASPs shall ensure that—
    a. relevant information is promptly communicated to all Staff; and
    b. any such updated operational policies and procedures are made available to all Staff at all times.

Part II – Tax Reporting and Compliance

1. VASPs must, at all times, comply with all tax reporting obligations under all applicable laws, regulations, rules or guidance as well as national, international and industry best practices, including under the United States Foreign Account Tax Compliance Act [**FATCA**] where applicable.

Part III – Anti-Money Laundering and Combating the Financing of Terrorism

Introduction

Part III of this Compliance and Risk Management Rulebook sets out requirements which aim to prevent the use of Virtual Assets and services relating to them in furtherance of illicit activities. VARA considers such illicit activities to include money laundering and the financing of terrorism, as well as proliferation financing and sanctions non-compliance.

A. Appointment and duties of Money Laundering Reporting Officer

1. VASPs shall appoint a Money Laundering Reporting Officer who—
   a. possesses at least two [2] years of experience handling AML/CFT matters; and
   b. is a Fit and Proper Person [**MLRO**].

   Such appointment shall be reviewed annually to ensure that the MLRO remains a Fit and Proper Person capable of discharging all relevant duties. VARA has the sole discretion to request a VASP to provide such evidence as VARA may require which shows that the above requirements are satisfied. In addition, VARA shall take into consideration any failures by an individual to comply with Part III of this Compliance and Risk Management Rulebook when assessing whether an individual is a Fit and Proper Person.
2. The MLRO shall be responsible for—
   a. ensuring the Board and Staff are properly and adequately trained in respect of their understanding and compliance with all applicable AML/CFT laws and regulatory requirements, particular those relevant to VA Activities;
   b. developing and implementing AML/CFT policies and procedures as required under Rule III.B of this Compliance and Risk Management Rulebook;
   c. conducting AML/CFT risk assessments in accordance with Rule III.D of this Compliance and Risk Management Rulebook and implementing all necessary changes to the VASP's relevant policies and procedures to address such issues and risks;
   d. monitoring and reporting Suspicious Transactions in accordance with Rule III.F of this Compliance and Risk Management Rulebook;

e. if necessary, ensuring appropriate corrective actions are taken in response to non-compliance with any Federal AML-CFT Laws;

f. reporting to the Board on a quarterly basis on the effectiveness of the VASP's AML/CFT policies and procedures, identifying any failures in such policies and procedures and/or any non-compliance with any Federal AML-CFT Laws;

g. ensuring the quarterly reports required under Rule III.A.2.f of this Compliance and Risk Management Rulebook include a summary of all Anonymity-Enhanced Transactions and clients involved during that quarter; and

h. making the reports required under Rule III.A.2.f of this Compliance and Risk Management Rulebook available to VARA on request.

3. AML/CFT activities may be delegated to appropriate Entities, provided that—

a. the MLRO shall continue to be held accountable for all responsibilities and obligations in relation to the implementation of the relevant policies and procedures; and

b. all applicable requirements in the Company Rulebook, including Outsourcing management requirements, are complied with.

4. Subject to relevant requirements in the Company Rulebook and if deemed appropriate by the VASP, the MLRO may hold more than one [1] non-client facing role within the VASP, provided such roles do not create conflicting duties, including but not limited to, the CO and the head of the risk function. VARA will take into account other roles held by the MLRO in determining whether the individual is a Fit and Proper Person.

B. Policies and procedures

1. VASPs will establish and implement policies and procedures to comply with all AML/CFT requirements and existing applicable laws, regulatory requirements and guidelines, including but not limited to—

a. the Federal AML-CFT Laws;

b. the Financial Action Task Force's [**FATF**] *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* [June 2020];

c. FATF's *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* [July 2021];

d. FATF's *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* [October 2021];

e. the *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations* [March 2022];

f. *Cabinet Resolution No. [74] of 2020 regarding the Terrorist List System and The Implementation of Security Council Resolutions Related to Preventing and Suppressing Terrorism and its Financing, Counter of Proliferation and its Financing, and the Relevant Resolutions;*

g. the UAE Executive Office for Control & Non-Proliferation [**EOCN**] *Guidance on Counter Proliferation Financing for FI's, DNFPBs, and VASPs* [March 2022]; and

h. the EOCN's Local Terrorist List, as may be amended from time to time.

2. To ensure compliance with the Federal AML-CFT Laws, such policies and procedures must establish courses of action allowing VASPs to—

a. refrain from opening or conducting any financial or commercial transaction under an anonymous or fictitious name or by pseudonym or number, and maintaining a relationship or providing any services to it;

b. ensure prompt application of the directives when issued by the competent authorities in the UAE for implementing United Nations Security Council Resolutions relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, and other related directives, as well as compliance with all other applicable laws, regulatory requirements and guidelines in relation to economic sanctions;

c. notwithstanding all relevant requirements in this Compliance and Risk Management Rulebook, maintain all records, documents, and data for all transactions, whether local or international, and make this information available to VARA upon request; and

d. ensure full compliance with any other AML/CFT requirements and applicable laws, regulatory requirements and guidelines as may be promulgated by VARA, UAE federal government bodies, FATF or the Middle East and North Africa Financial Action Task Force from time to time.

3. VASPs shall establish adequate risk rules to screen clients, UBOs, Virtual Asset transactions and VA Wallet addresses to—
   a. identify potential illicit activities, potentially adverse information in higher risk situations [e.g. criminal history] and applicability of targeted or other international financial sanctions; and
   b. alert operation and compliance teams to impose relevant restriction and conduct further investigation.
4. All policies and procedures established and implemented pursuant to Rule III.B.1 of this Compliance and Risk Management Rulebook must be attested by a competent third party and shall be submitted to VARA in the licensing process and no more than twenty-one [21] calendar days after any changes coming into effect.

C. AML/CFT controls

1. VASPs should have effective AML/CFT controls and systems in place which can adequately manage the AML/CFT risks relevant to their VA Activities, including the use of distributed ledger analytics tools, as well as other investigative tools or capabilities to monitor and screen transactions.
2. In respect of any distributed ledger analytics tools used, VASPs should review and document their review of the capabilities and weaknesses of such tools and design controls to monitor clients' interaction with their VA Activities.
3. Information about Virtual Asset transactions and VA Wallet addresses are dynamic in nature. VASPs should review and document their review of the performance and function of any distributed ledger analytics tools used to for ongoing monitoring.
4. VASPs shall, if applicable, implement internal controls to address the *FATF Report Virtual Assets Red Flags Indicators of Money Laundering and Terrorist Financing* [September 2020] when designing transaction monitoring scenarios and thresholds to monitor clients' interaction with their VA Activities.

D. Risk assessment

1. In implementing adequate and appropriate AML/CFT policies, procedures, and controls to detect and prevent illicit activities, VASPs must conduct AML/CFT business risk assessments.
2. The AML/CFT business risk assessments must be designed and implemented to assist VASPs to better understand their risk exposure and areas in which they should prioritise allocation of resources in their AML/CFT activities. This includes identifying and assessing the AML/CFT risks in relation to the development and use of new or existing—
    a. Virtual Assets [in particular, Anonymity-Enhanced Cryptocurrencies];
    b. Virtual Asset related products or services [in particular, methods in which Anonymity-Enhanced Transactions can be conducted];
    c. Virtual Asset related business and professional practices; and
    d. technologies associated with VA Activities.
3. VASPs enabling Anonymity-Enhanced Transactions as part of their VA Activities must implement proportionately enhanced controls to ensure compliance with all applicable laws and regulations [including all Federal AML-CFT Laws], Regulations, Rules and Directives, as well as effectively monitor and prevent illicit uses. Such controls shall include conducting enhanced CDD on each client using those services, which shall be verified every six [6] months. In the case where the AML/CFT risks cannot be adequately mitigated, such products or services should not be offered.

E. Client due diligence

1. VASPs shall adopt a risk-based application of CDD measures in accordance with the Federal AML-CFT Laws.
2. VASPs are required to undertake CDD measures to verify the identity of the client and the UBO[s] before or during the establishment of a business relationship for the purposes of providing services relating to VA Activities, or before executing a transaction [whether or not denominated in Virtual Assets] for a client with whom there is no business relationship.
3. VASPs shall undertake CDD measures in the following circumstances—
    a. when establishing a business relationship with a client for the purposes of providing services relating to VA Activities;

b. when carrying out occasional transactions in favour of a client for amounts equal to or exceeding AED 3,500, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;

c. where there is an instruction from a client to handle a potential Suspicious Transaction;

d. where there are doubts about the veracity or adequacy of previously obtained identification information of a client; and

e. when carrying out any transaction for high-risk clients as characterised in the Federal AML-CFT Laws.

4. VASPs should undertake CDD measures in their ongoing supervision of business relationships with clients, including—

a. auditing transactions that are carried out throughout the period of the business relationship, to ensure that the transactions conducted are consistent with the information on file regarding clients and the risks they pose, including, where necessary, the source of funds; and

b. ensuring that the documents, data or information obtained from CDD measures are up-to-date and appropriate by regularly reviewing such records, particularly those of high-risk clients as characterised in the Federal AML-CFT Laws.

5. As part of the CDD process, VASPs shall verify clients' identity by reference to the following documents, data or information from a reliable and independent source—

a. *For individuals*—

i. full name as shown on an identification card or a travel document [along with a copy of the original and valid identification card or travel document];

ii. nationality;

iii. address;

iv. place of birth;

v. name and address of employer; and

vi. if the client is a Politically Exposed Person, approval from the MLRO and a member of the Senior Management is required prior to establishing a business relationship with such client.

b. *For Entities which are not individuals*—

i. full name of the Entity;

ii. type of Entity;

iii. constitutional documents [e.g. memorandum of association and articles of association] attested by competent authorities within the UAE;

iv. principle place of business;

v. names of individuals holding Senior Management positions in the Entity; and

vi. if the UBO is a Politically Exposed Person, approval from the MLRO and a member of the Senior Management is required prior to establishing a business relationship with such client.

6. VASPs are further required to—

a. verify that any Entity purporting to act on behalf of the client is so authorised, and verify the identity of that Entity in accordance with Rule III.E.5 of this Compliance and Risk Management Rulebook;

b. understand the intended purpose and nature of the business relationship with the client, and obtain, when necessary, information related to this purpose; and

c. where the VASP's client is a business or otherwise provides services to other clientele, understand the nature of the client's business as well as the client's ownership and control structure, including but not limited to the following—

i. the identity of UBO[s];

ii. whether such structure includes any DAOs and, if so, the intended purpose of such DAOs;

iii. the type, nature and pursuits of the clientele of a prospective client and where necessary carry out appropriate due diligence on the client's clientele in order to ensure compliance with the Federal AML-CFT Laws.

7. If a VASP is unable to conduct appropriate CDD on a client, it shall not—

a. establish or maintain a business relationship with such client; or

b. execute any transaction for such client.

8. If a VASP relies on third parties to perform CDD, it shall remain liable for ensuring such third parties perform CDD in accordance with all relevant Rules and Directives. VASPs that rely on

third parties to undertake CDD on their behalf must therefore implement adequate measures in keeping with the nature and size of their businesses [including VA Activities] to ensure that such third parties' performance of CDD is in accordance with all relevant Rules and Directives.

F. Suspicious Transaction monitoring and reporting

1. VASPs shall employ methods which are appropriate to their particular circumstances and VA Activities to continuously monitor business relationships with clients to identify any Suspicious Transactions. Such methods shall ensure that no "tipping-off" or similar offence occurs. Such methods shall also ensure all Suspicious Transactions are immediately reported to the MLRO, in order for the MLRO to meet the requirements of this Rule III.F. VASPs are required to document, obtain Senior Management approval for, and periodically review and update such methods to ensure their effectiveness.
2. VASPs shall put in place and regularly update indicators that can be used to identify possible Suspicious Transactions.
3. Upon suspicion or reasonable grounds to suspect that the proceeds of a transaction are related to a crime, or the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime, the MLRO shall be responsible for—
   a. immediately reporting to the UAE FIU and VARA such Suspicious Transactions in accordance with Rule III.F.4 of this Compliance and Risk Management Rulebook;
   b. responding to all additional information requests from the UAE FIU and/or VARA promptly and in any event within forty-eight [48] hours of such requests;
   c. undertaking any additional actions as may be requested by the UAE FIU and/or VARA within any specified timeframe in such requests; and
   d. in the event the MLRO is not the same individual as the CO, immediately reporting to the CO that a Suspicion Transaction report has been made, provided that the provision of any such report would not be considered "tipping-off" or a similar offence under any applicable laws or regulations.
4. All reports regarding Suspicious Transactions shall be made—
   a. to the UAE FIU and VARA on the GoAML platform or by any other means approved by the UAE FIU and/or VARA; and

b. in accordance with any Guidance which may be issued by VARA from time to time.

5. VASPs shall continue monitoring [on a near real time basis where appropriate] any transactions which are the subject of a Suspicious Transaction report.

G. FATF Travel Rule

1. Prior to initiating any transfer of Virtual Assets with an equivalent value exceeding AED 3,500, VASPs must obtain and hold required and accurate originator information and required beneficiary information and make it available on request to VARA and/or other appropriate authorities.
2. Prior to permitting any clients access to Virtual Assets received from a transfer with an equivalent value exceeding AED 3,500, a beneficiary VASP must obtain and hold required originator information and required and accurate beneficiary information and make it available on request to VARA and/or other appropriate authorities.
3. Required originator information shall include, but not be limited to, the originator's—
   a. name;
   b. account number or VA Wallet address; and
   c. residential or business address.
4. Required beneficiary information shall include, but not be limited to, the beneficiary's—
   a. name; and
   b. account number or VA Wallet address.
5. Prior to entering into any transaction with a counterparty VASP or virtual asset service provider in any other jurisdiction, VASPs must complete risk-based due diligence on such counterparty in order to mitigate AML/CFT risks. This due diligence does not need to be completed for every subsequent transaction with the counterparty unless a heightened counterparty risk is assessed or identified.
6. In complying with the Travel Rule, VASPs must consider how they will handle the risks associated with—
   a. deposits or withdrawals [including those which are compliant with the Travel Rule and those which are not];
   b. non-obliged entities [i.e. unhosted VA Wallets]; and

c. Anonymity-Enhanced Transactions.

7. VASPs shall be required to demonstrate to VARA how they comply with the Travel Rule during the licensing process and submit to VARA relevant policies and controls. VASPs should also include their plan to comply with the Travel Rule with virtual asset service providers in jurisdictions where the Travel Rule is not a legislative requirement [i.e. the "sunrise issue"].

8. In implementing policies and controls to comply with the Travel Rule and AML/CFT Rules, VASPs shall be guided by *FATF Interpretive Note to Recommendation 15* and all applicable laws, regulatory requirements and guidelines as may be in force from time to time. VASPs must monitor for any transaction or series of transactions that seeks to circumvent any regulatory thresholds to bypass Travel Rule requirements.

9. VARA may require VASPs to report on their compliance with the Travel Rule and the effectiveness of their implementing policies and controls, at any time.

H. Record keeping

1. VASPs shall retain the following types of records relating to AML/CFT in accordance with the Federal AML-CFT Laws—

   a. Virtual Asset transaction records, including operational and statistical records, documents and information [whether or not recorded on public distributed ledgers] concerning all transactions executed or processed by the VASP;

   b. CDD records, including records, documents, and information about clients [e.g. account files and business correspondence], and results from the investigation and analysis of clients' activities;

   c. information relating to third parties engaged by the VASP to undertake CDD;

   d. records relating to ongoing monitoring of business relationships with clients; and

   e. Suspicious Transaction reports made in accordance with Rule III.F of this Compliance and Risk Management Rulebook.

2. VASPs shall retain all records required in Rule III.H.1 for a period of no less than eight [8] years.

I. Enforcement

1. VASPs which fail to comply with Rules in this Part III of this Compliance and Risk Management Rulebook may be subject to enforcement actions taken by VARA or other penalties as set out in the Regulations and the Federal AML-CFT Laws.

Part IV – Client Money Rules

Application and Interpretation

1. **Client Money** means all money held or controlled by a VASP on behalf of a client in the course of, or in connection with, the carrying on of any VA Activity, except for—
   a. money which is immediately due and payable to a VASP for the VASP's own account, such as fees for services provided to a client;
   b. amounts payable by the VASP for expenses incurred on behalf of the client; and
   c. other charges that are due and payable to the VASP.
2. Client Money does not include any Virtual Assets held by a VASP on behalf of a client.
3. Client Money is held or controlled by a VASP if it is—
   a. directly held by the VASP;
   b. held in an account in the name of the VASP; or
   c. held by an Entity, or in an account in the name of an Entity, controlled by the VASP.
4. **Client Account** means an account at a Third-Party Bank which—
   a. holds or is established to hold the Client Money of one or more clients; and
   b. is maintained in the name of the VASP.
5. **Third-Party Bank** means the bank with which a Client Account is maintained.

A. Treatment of Client Money

1. VASPs must have in place the necessary policies, systems and controls, appropriate to the nature and scale of their operations, to ensure compliance with this Part IV of this Compliance and Risk Management Rulebook.
2. VASPs holding Client Money must hold it on trust for their clients in a Client Account.
3. All Client Accounts must include the words "Client Account" in their title.
4. VASPs must have systems and controls to ensure that the Client Money is identifiable and secure at all times.
5. Where a VASP holds or controls Client Money it must ensure—
   a. except where otherwise provided in Rule IV.A.6 of this Compliance and Risk Management Rulebook, that the Client Money is paid into a Client Account within one [1] calendar day of receipt;

b. Client Money held or controlled on behalf of clients in the UAE is paid into Client Accounts maintained with Third-Party Banks in the UAE; and

c. Client Money held or controlled on behalf of clients outside of the UAE may be deposited into Client Accounts with Third-Party Banks outside of the UAE but must be moved to, and maintained with, Third-Party Banks in the UAE and VASPs must initiate such moves within twenty-four [24] hours of receipt.

6. The requirement for a VASP to pay Client Money into a Client Account does not, subject to Rule IV.A.7 of this Compliance and Risk Management Rulebook, apply with respect to such Client Money—

a. temporarily held by the VASP before forwarding to an Entity nominated by the client;

b. in connection with a delivery versus payment transaction where—

i. in respect of a client purchase, Client Money from the client will be due to the VASP within one [1] calendar day upon the fulfilment of a delivery obligation; or

ii. in respect of a client sale, Client Money will be due to the client within one [1] calendar day following the client's fulfilment of a delivery obligation; or

iii. held in the client's own name where the VASP has a mandate to manage the Client Money on a discretionary basis.

7. VASPs must pay Client Money of the type described in Rule IV.A.6.b of this Compliance and Risk Management Rulebook into a Client Account where they have not fulfilled their delivery or payment obligation within three [3] calendar days of receipt of the Client Money.

8. VASPs must maintain adequate records of all payments of Client Money received including, in respect of each payment, the—

a. date of receipt;

b. name and unique identifier of the client for whom payment is to be credited;

c. name of the Entity who made the payment;

d. transaction identifier and/or reference; and

e. date when the payment was presented to the VASP's Third-Party Bank.

9. Payment into Client Accounts.

a. VASPs must maintain systems and controls for identifying money which must not be in a Client Account and for transferring it without delay.

b. VASPs must not hold or deposit their own money into a Client Account, except where—

i. it is a minimum sum required to open the account, or to keep it open;

ii. the money is received by way of mixed remittance, provided the VASP transfers out that part of the payment which is not Client Money within one [1] calendar day of the day on which the VASP would normally expect the remittance to be cleared;

iii. interest credited to the account exceeds the amount payable to clients, as applicable, provided that the money is removed within twenty [20] calendar days; or

iv. it is to meet a temporary shortfall in Client Money.

10. Payment out of Client Accounts.

a. VASPs must have procedures for ensuring all withdrawals from a Client Account are authorised.

b. Client Money must remain in a Client Account until it is—

i. due and payable to the VASP;

ii. paid to the client on whose behalf the Client Money is held;

iii. paid in accordance with a client's instruction on whose behalf the Client Money is held;

iv. required to meet the payment obligations of the client on whose behalf the Client Money is held; or

v. paid out in circumstances that are otherwise authorised by VARA.

c. VASPs must not use Client Money belonging to one client to satisfy an obligation owed to another client, nor for any other obligation owed to other Entities [including but not limited to for liquidity, capital ratios or their own balance sheet purposes].

d. VASPs must have a system for ensuring no off-setting or debit balances occur in Client Accounts.

B. Third-Party Bank

1. VASPs may only maintain Client Accounts at Third-Party Banks appropriately and validly authorised to accept or take deposits in accordance with applicable laws and regulatory requirements in the relevant jurisdiction and which must not be in the same Group as the VASP.

2. Payment of Client Money to a Third-Party Bank.

   a. VASPs may only pass, or permit to be passed, Client Money to a Third-Party Bank if—

      i. the Client Money is to be used in respect of a transaction or series or transactions for that client; and

      ii. the Third-Party Bank is appropriately and validly authorised to accept or take deposits in accordance with applicable laws and regulatory requirements in its relevant jurisdiction as per Rule IV.B.1 of this Compliance and Risk Management Rulebook.

3. When a VASP opens a Client Account with a Third-Party Bank it must promptly obtain a written acknowledgement from the Third-Party Bank stating that—

   a. all money standing to the credit of the account is held by the VASP as agent and that the Third-Party Bank is not entitled to combine the account with any other account or to exercise any charge, mortgage, lien, right of set-off or counterclaim against money in that account in respect of any sum owed to it on any other account of the VASP; and

   b. the title of the account sufficiently distinguishes that account from any account containing money that belongs to the VASP, and is in the form requested by the VASP.

4. If the Third-Party Bank does not promptly provide the acknowledgement referred to in Rule IV.B.3 of this Compliance and Risk Management Rulebook, the VASP must refrain from making further deposits of Client Money with that Third-Party Bank and withdraw any Client Money in that Client Account.

C. Disclosure, reporting and audit requirements

1. Proper record keeping.

   a. VASPs shall keep proper and up-to-date records regarding—

      i. the receipt and payment of Client Money and in and out of Client Accounts; and

      ii. movements of Client Money within internal systems

to enable the reconciliation of any differences in balances or positions of Client Money.

b. VASPs shall have appropriate procedures for identifying Client Money received. The procedures should cover Client Money received through all means, including electronically or via agents of the VASP [e.g. banks, payment processors].

c. VASPs may be requested to demonstrate evidence of above records upon VARA's request.

2. Client reporting.

a. VASPs must send or otherwise make available a statement to clients at least monthly, or as agreed with the client, which shall include—

i. the client's total Client Money balances held by the VASP;

ii. the amount, date and value of each credit and debit paid into and out of the account since the previous statement; and

iii. any interest earned or charged on the Client Account since the previous statement.

b. The statement sent to the client must be prepared within twenty-five [25] calendar days of the statement date.

D. Reconciliation

1. VASPs must maintain a system to ensure that accurate reconciliations of the Client Accounts are carried out daily. The reconciliation must include—

a. a full list of individual client credit ledger balances, as recorded by the VASP;

b. a full list of individual client debit ledger balances, as recorded by the VASP;

c. a full list of outstanding lodgements;

d. a full list of Client Account cash book balances; and

e. formal statements from Third-Party Banks showing account balances as at the date of reconciliation.

2. VASPs must—

a. reconcile the individual credit ledger balances, Client Account cash book balances, and the Third-Party Bank Client Account balances;

b. check that the balance in the Client Accounts as at the close of business on the previous day was at least equal to the aggregate balance of individual credit ledger balances as at the close of business on the previous day; and

c. ensure that all shortfalls, excess balances and unresolved differences, other than differences arising solely as a result of timing differences between the accounting systems of the Third-Party Bank and the VASP, are investigated and, where applicable, corrective action taken as soon as possible, including where necessary using the VASP's own funds.

3. VASPs must perform the reconciliations in Rule IV.D.2 of this Compliance and Risk Management Rulebook on a daily basis.

4. VASPs must ensure that the process of reconciliation does not give rise to a conflict of interest.

5. VASPs must notify VARA where there has been a material discrepancy with the reconciliation which has not been rectified.

E. Failure to comply

1. VASPs which become aware that they do not comply with any Rules in this Part IV of this Compliance and Risk Management Rulebook must notify VARA in writing of any such non-compliance within one [1] calendar day.

2. Failure to comply with any Rules in this Part IV of this Compliance and Risk Management Rulebook may result in VARA taking appropriate enforcement action[s] as it deems fit and the VASP must comply with all corrective action[s] as instructed by VARA.

Part V – Client Virtual Assets Rules

Application and Interpretation

1. **Client VAs** means all Virtual Assets held or controlled by a VASP on behalf of a client in the course of, or in connection with, the carrying on of any VA Activity, except for—
   a. Virtual Assets immediately due and payable to a VASP for the VASP's own account, such as fees for services provided to a client;
   b. amounts payable by the VASP for expenses incurred on behalf of the client; and
   c. other charges that are due and payable to the VASP.
2. Client VAs are held or controlled by a VASP if they are—
   a. directly held by the VASP in an account or VA Wallet;
   b. held in an account or VA Wallet in the name of the VASP;
   c. held by a legal entity, or in an account or VA Wallet in the name of a legal entity, controlled by the VASP; or
   d. the private keys and/or seed phrase of the VA Wallet are held or controlled by the VASP.

A. Treatment of Client VAs

1. VASPs must have in place the necessary policies, systems and controls, appropriate to the nature and scale of their operations, to ensure compliance with this Part V of this Compliance and Risk Management Rulebook.
2. Client VAs are not depository liabilities or assets of the VASP.
3. VASPs shall hold Client VAs in separate VA Wallets from all Virtual Assets of the VASP.
4. VASPs must hold Client VAs on a one-to-one basis and shall not authorise or permit rehypothecation of Client VAs, unless they have explicit prior consent from the client providing discretionary authority to do so, and are appropriately authorised and Licensed by VARA to carry out all relevant VA Activity[ies] in respect of such Virtual Assets.
5. All proceeds related to Client VAs, such as "airdrops", "staking gains" or similar proceeds shall accrue to the client's benefit, unless the VASP has the client's prior consent specified in a written agreement with the client or otherwise. VASPs may decide not to collect or distribute certain proceeds, including where such proceeds are below a value to be determined by the VASP,

provided that the VASP has disclosed this to the client and obtained acceptance in accordance with all applicable laws.

B. Proof of reserves

1. In addition to the Reserve Assets requirements in the Company Rulebook, VASPs shall comply with all requirements stipulated by VARA from time to time, including as part of a VASP's licensing process, in order to demonstrate that assets held in reserve cover all of their liabilities with respect to Client VAs.

C. Reconciliation

1. VASPs must maintain a system to ensure that accurate reconciliations of the Virtual Assets owned by each client are carried out daily. The reconciliation must include—
   a. a full list of individual client credit ledger balances, as recorded by the VASP; and
   b. a full list of individual client debit ledger balances, as recorded by the VASP.
2. VASPs must notify VARA where there has been a material discrepancy with the reconciliation which has not been rectified.

Part VI – Anti-Bribery and Corruption

A. General principles

1. VASPs shall establish and maintain an effective anti-bribery and corruption policy to ensure that the Board and all Staff must comply with all applicable laws and regulations relevant to anti-bribery and corruption in all jurisdictions in which they operate. Such policy must allow for reports to be made by Entities outside of the VASP and protect the identity and confidentiality of the Entity who has made a report at all times.
2. VASPs must conduct all business in an honest and ethical manner and must take a zero-tolerance approach to bribery and corruption. The Board and all Staff must act professionally, fairly and with integrity in all business dealings and relationships.
3. It is prohibited for any VASP, members of the Board and all Staff, to—
   a. give, promise to give, or offer, a payment, gift or hospitality to a third party or otherwise engage in or permit a bribery offence to occur, with the expectation or hope that an advantage in business will be received or to reward a business advantage already given;
   b. give, promise to give, or offer, a payment, gift or hospitality to a third party to facilitate or expedite a routine procedure;
   c. accept a payment, gift or hospitality from a third party if it knows or suspects that such payment, gift or hospitality is offered or provided with an expectation that a business advantage will be provided by the VASP in return;
   d. threaten or retaliate against another member of the Board or Staff who has refused to commit a bribery offence or who has raised concerns; and
   e. engage in any activity that might lead to a breach of the anti-bribery and corruption Rules in this Part VI of this Compliance and Risk Management Rulebook.
4. The anti-bribery and corruption Rules in this Part VI of this Compliance and Risk Management Rulebook do not prohibit normal and appropriate hospitality [given or received in accordance with the VASP's own gifts and hospitality policy] to or from third parties, provided relevant policies are compliant with applicable laws. Such gifts and hospitality policy should set out clearly what is and is not appropriate to make or receive gifts and/or hospitality to and from a third party.

5. The CO will monitor the effectiveness of the anti-bribery and corruption policy on a regular basis. Any deficiencies identified should be dealt with as soon as possible.

B. No corrupt payments

1. It is prohibited for any VASP or any members of its Board, Staff, consultants or contractors, any Group company, agent, business partner, contractor or supplier of the VASP to make any payment[s] to a third party where there is any reason to believe that all or any part of such payment will go towards a bribe or otherwise facilitate any corruption.
2. All payments made by VASPs for services must be appropriate and justifiable for the purpose of legitimate services provided.

C. Investigation and reporting

1. VASPs must establish, maintain and publish methods of contact including, but not limited to, a telephone line, for receiving reports of any violation or possible violation of any applicable laws and regulations relevant to anti-bribery and corruption by the VASP, or its Board or Staff on its behalf.
2. Any member of the Board or Staff must report to the CO as soon as possible if they believe or suspect that an action in conflict with the anti-bribery and corruption Rules in this Part VI of this Compliance and Risk Management Rulebook has occurred, or may occur, or has been solicited by any other Entity.
3. The CO shall investigate any report of a violation or possible violation of the anti-bribery and corruption Rules in this Part VI of this Compliance and Risk Management Rulebook and shall follow the below procedures—
    a. An investigation file should be opened. In the case of an oral report, the CO should prepare a written summary.
    b. The CO shall appoint an independent Entity who shall promptly commission the conduct of an investigation. The investigation will document all relevant facts, including Entities involved, times and dates.
    c. The CO shall advise the Board of the existence of an investigation.

d. The identity of the individual disclosing relevant information to the CO should be treated in accordance with applicable UAE laws and regulations.

e. On completion of the investigation, a written investigation report will be provided by the Entity employed to conduct the investigation to the CO. If any unlawful conduct is found, the CO must advise the Board accordingly.

f. If any unlawful conduct is found, the VASP shall take such remedial action as the Board deems appropriate to achieve compliance with its internal anti-bribery and corruption policy and all applicable anti-bribery and corruption laws. The Entity employed to conduct the investigation shall prepare a written summary of the remedial actions taken.

g. The written investigation report and a written summary of the remedial actions taken shall be retained by the CO for a period of no less than eight [8] years from completion of the remedial action. Such reports shall be made available to VARA upon request.

D. Information and trainings

1. VASPs shall implement and provide an anti-bribery and corruption training programme for the Board and all Staff on a regular basis and monitor their compliance with all established procedures. All members of the Board and Staff must participate in all such trainings provided by the VASP.

2. VASPs shall ensure that all members of the Board and Staff to have full access at all times to the most up-to-date anti-bribery and corruption policy and will be informed of any changes to such policy.

3. Training on the anti-bribery and corruption policy should form part of the induction programme made available to all new Board members and Staff.

4. In addition to relevant requirements in the Market Conduct Rulebook, a zero-tolerance approach to bribery and corruption and all relevant policies must be disclosed by all VASPs to the public and communicated at the outset of all business relationships as appropriate.

E. Responsibility for the policy

1. The Board shall have the overall responsibility for ensuring its anti-bribery and corruption policy is up-to-date and complies with all applicable laws and regulations in all jurisdictions where the VASP conducts its business.
2. The CO has the primary and day-to-day responsibility for implementing the anti-bribery and corruption policy and for monitoring its effectiveness.

F. Consequences of breach

1. Failure to comply with a VASP's anti-bribery and corruption policy should result in severe consequences, including internal disciplinary action and termination of employment without notice.
2. VASPs should immediately report to VARA any finding of unlawful conduct in breach of the anti-bribery and corruption Rules in this Part VI of this Compliance and Risk Management Rulebook.

Schedule 1 – Definitions

Term	Definition
"AML/CFT"	has the meaning ascribed to it in the Regulations.
"Anonymity-Enhanced Cryptocurrencies"	has the meaning ascribed to it in the Regulations.
"Anonymity-Enhanced Transactions"	means transactions denominated in Virtual Assets which are not Anonymity-Enhanced Cryptocurrencies, but which prevent the tracing of transactions or record of ownership.
"BCDR Plan"	means the Business Continuity and Disaster Recovery Plan of a VASP.
"Board"	has the meaning ascribed to it in the Company Rulebook.
"Capital and Prudential Requirements"	has the meaning ascribed to it in the Company Rulebook.
"CDD"	means client due diligence, including but not limited to due diligence on the clientele of a VASP's client.
"Client Account"	has the meaning ascribed to it in Part IV of this Compliance and Risk Management Rulebook.
"Client Money"	has the meaning ascribed to it in Part IV of this Compliance and Risk Management Rulebook.
"Client VA"	has the meaning ascribed to it in Part V of this Compliance and Risk Management Rulebook.
"CMS"	means the compliance management system of a VASP.
"Compliance Officer" or **"CO"**	has the meaning ascribed to it in Part I of this Compliance and Risk Management Rulebook.
"Company Rulebook"	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
"Compliance and Risk Management Rulebook"	means this Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.

Term	Definition
"Controlling Entity"	has the meaning ascribed to it in the Company Rulebook.
"Decentralised Autonomous Organisation" or **"DAO"**	has the meaning ascribed to it in the Company Rulebook.
"Directive"	has the meaning ascribed to it in the Regulations.
"Dubai VA Law"	means *Law No. [4] of 2022 Regulating Virtual Assets in the Emirate of Dubai*, as may be amended from time to time.
"Emirate"	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
"Entity"	means any legal entity or individual.
"EOCN"	means the UAE Executive Office for Control & Non-Proliferation.
"FATCA"	means the United States *Foreign Account Tax Compliance Act*.
"FATF"	means the Financial Action Task Force.
"Federal AML-CFT Laws"	has the meaning ascribed to it in the Regulations.
"Fit and Proper Person"	means an individual who complies with all fit and proper requirements in the Company Rulebook.
"GoAML"	means the electronic platform through which Suspicious Transaction reports can be submitted to the UAE FIU.
"Group"	has the meaning ascribed to it in the Company Rulebook.
"Guidance"	has the meaning ascribed to it in the Regulations.
"Inside Information"	has the meaning ascribed to it in the Regulations.
"Insolvency Proceedings"	has the meaning ascribed to it in the Regulations.
"Licence"	has the meaning ascribed to it in the Regulations.
"Licensed"	means having a valid Licence.
"Market Conduct Rulebook"	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.

Term	Definition
"Money Laundering Reporting Officer" or **"MLRO"**	has the meaning ascribed to it in Rule III.A.1 of this Compliance and Risk Management Rulebook.
"Outsourcing"	has the meaning ascribed to it in the Company Rulebook.
"Politically Exposed Person" or **"PEP"**	has the meaning ascribed to it in the Company Rulebook.
"PDPL"	means the *Federal Decree-Law No. [45] of 2021 on the Protection of Personal Data*.
"Personal Data"	has the meaning ascribed to it in the PDPL.
"Regulations"	means the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time.
"Related Parties"	has the meaning ascribed to it in the Company Rulebook.
"Reserve Assets"	has the meaning ascribed to it in the Company Rulebook.
"Responsible Individuals"	has the meaning ascribed to it in the Company Rulebook.
"Rule"	has the meaning ascribed to it in the Regulations.
"Rulebook"	has the meaning ascribed to it in the Regulations.
"Senior Management"	has the meaning ascribed to it in the Company Rulebook.
"Staff"	has the meaning ascribed to it in the Company Rulebook.
"Suspicious Transaction"	means any transaction, attempted transaction, or funds which a VASP has reasonable grounds to suspect as constituting, in whole or in part, and regardless of the amount or the timing, any of the following— [a] the proceeds of crime [whether designated as a misdemeanour or felony, and whether committed within the Emirate or in another country in which it is also a crime]; [b] being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations; and [c] being intended to be used in an activity related to such crimes.

Term	Definition
"Technology and Information Rulebook"	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
"Third-Party Bank"	has the meaning ascribed to it in Part IV of this Compliance and Risk Management Rulebook.
"Travel Rule"	has the meaning ascribed to it in FATF's *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers* [October 2021], as may be amended from time to time.
"UAE"	means the United Arab Emirates.
"UAE FIU"	means the UAE Financial Intelligence Unit.
"Ultimate Beneficial Owner" or "**UBO**"	has the meaning ascribed to it in the Company Rulebook.
"VA Activity"	means the activities listed in Schedule 1 of the Regulations, as may be amended from time to time.
"VA Wallet"	has the meaning ascribed to the term "Virtual Asset Wallet" in the Dubai VA Law.
"VARA"	means the Dubai Virtual Assets Regulatory Authority.
"VASP"	means an Entity Licensed by VARA to conduct VA Activity[ies] in the Emirate.
"Virtual Asset" or **"VA"**	has the meaning ascribed to it in the Dubai VA Law.