

VARA Rulebooks V2.0

Please note that the below is intended to be an illustrative commentary and not to constitute legal advice. The amendments to the VARA Rulebooks are extensive, and we strongly recommend that any readers of this article seek independent counsel before carrying out any virtual asset services in the territory of the UAE.

High Impact Changes

Regulatory Updates

Procedural Changes

Company Rulebook - Changes and Impact

Rule VI. B.1

The amendment formally designates Category 1 VA Issuance as a distinct licensed activity under the regulatory framework and capital requirement is to be determined in line with the VA Issuance Rulebook of the relevant Annex.

Impact

This establishes clearer licensing and capital requirements for VA Issuance.

Rule III. F.2

The revised clause adds:

"...and any measures or controls the individual and/or the VASP will have in place in response to such conviction."

This addition broadens the assessment criteria for determining whether an individual with a prior conviction from any jurisdiction (UAE or otherwise) may still qualify as a "Fit and Proper Person."

Impact

This is a relevant update, considering the recent high-profile convictions of founders/senior members of large crypto firms. It is important to note, however, that the amendment doesn't nullify a conviction, it simply asks whether the convicted party has learned, adapted, and instituted guardrails. It gives regulators discretion to contextualise.

Company Rulebook - Changes and Impact

Rule VII. A. 1. & I AND Rule VII. A. 2

The new provision mandates that all VASPs must maintain, update, and be prepared to always implement a Wind Down Plan, regardless of solvency or operational intent.

Impact

This establishes clearer licensing and capital requirements for VA Issuance.

Key features of the updated requirements include:

- (i) Client Asset Protections: VASP must ensure that the sale of Client's Money and Client's Virtual Assets are explicitly excluded from any sale or transfer arising from wind-down, insolvency proceedings or otherwise from the sale of the VASP.
- (ii) Regulatory Intervention Rights: VARA has the power to intervene in or assume control over Client's Money and Client's Virtual Assets at its discretion in cases of non-compliance or otherwise. VASPs must ensure their systems and legal contracts enable the ability of VARA to undertake such intervention when VARA deems it necessary.
- (iii) Voluntary Exit Protocol: VASPs voluntarily exiting the market (i.e., not when it is insolvent or subject to insolvency proceedings) must notify VARA within one day of making such decision, submit their current Wind Down Plan, comply with any modifications required by VARA, and provide weekly progress reports along with all the updates as requested, during the week of implementation of Wind Down Plan.

Company Rulebook - Changes and Impact

Rule II. C. 2.b AND Rule IV. A.3.c

The term "*Chinese Walls*" has been replaced with the culturally neutral term "*Information Barriers*." This revision is purely semantic and does not affect the substantive legal framework.

"*Information Barriers*" continues to encompass the same legal and compliance expectations, including:

(i) **Physical Barriers:** Segregated teams, restricted office zones, and secure physical access to prevent unauthorized interactions.

Impact

This change reflects a commitment to inclusive language without altering regulatory standards or obligations.

(ii) **Digital Barriers:** Robust IT controls such as access restrictions, encryption, and firewalls to safeguard sensitive data.

(iii) **Procedural Barriers:** Codified policies, training, monitoring, and independent audits to uphold the integrity of internal separations.

Rule III. G.2

VARA is now expressly empowered to direct VASPs to implement additional controls or take any other necessary actions when an individual is no longer deemed Fit and Proper. This was earlier limited to imposition of punitive measures and fines.

Impact

The amendments reflect a deliberate shift from a purely punitive approach to one that incorporates corrective and risk-mitigation measures that can be imposed by the regulator.

Compliance & Risk Management Rulebook - Changes and Impact

Rule III.D.2

The amendment introduces two new categories under AML/CFT risk assessments:

- (i) risks arising from the development or use of technologies not specific to virtual assets, such as artificial intelligence and machine learning; and
- (ii) a catch-all category for other emerging risks.

Impact

These changes extend VASPs' compliance perimeter to cover indirect but material threats. AI and machine learning may be used to automate illicit transactions, create synthetic identities, or manipulate market behaviour. Deepfake technology enables identity fraud and onboarding breaches. Quantum computing threatens the integrity of encryption protocols that underpin wallet security and transaction confidentiality.

Impact

Of particular concern is the emergence of autonomous AI agents capable of initiating economic activity with minimal or no human oversight. Within decentralised systems, where the distinction between actor and platform is already fluid, such agents raise unresolved questions of accountability in cases of AML/CFT breaches.

Further, the residual category compels VASPs to identify and mitigate risks from rapidly evolving technologies, even before concrete typologies emerge. This ensures AML/CFT controls remain adaptive and anticipatory in a landscape defined by innovation-driven risk.

Compliance & Risk Management Rulebook - Changes and Impact

Rule III.D.3–8

Under Rule III.D.3, VASPs must conduct business risk assessments at least quarterly, and in response to any material change triggered by a significant incident.

Rule III.D.4 requires that AML/CFT policies, procedures, systems, and resource allocations be demonstrably informed and updated based on these business risk assessments.

Impact

VARA has significantly strengthened its risk governance framework through amendments to Rules III.D.3–8, embedding more prescriptive obligations on VASPs.

This reflects VARA's recognition that risk exposure varies significantly across client types (e.g. retail vs. institutional, geographies, transaction volumes), and that a "one-size-fits-all" approach is inadequate in addressing complex financial crime risks in the crypto sector.

Rules III.D.6–8 introduce mandatory quarterly client risk assessments across the entire client base for AML/CFT purposes. VASPs must:

- (i) Formalise risk categorisation criteria and tiering methodologies, based on both severity and likelihood of occurrence;
- (ii) Develop documented policies outlining how assessments are conducted, implemented, and followed up; and
- (iii) Maintain comprehensive audit trails evidencing risk mitigation actions and decision-making processes.

Compliance & Risk Management Rulebook - Changes and Impact

Rule III.B.1.f

The amendment to remove the previous explicit reference to Cabinet Resolution No. [74] of 2020 concerning the Terrorist List System and the implementation of UN Security Council resolutions on counterterrorism, counter-proliferation, and related financial sanctions.

Impact

While the requirement for VASPs to comply with all applicable AML/CFT laws remains, this change appears to be a case of legislative consolidation. Moreover, by removing granular references, the provision becomes future proof, avoiding the need for continuous updates in response to evolving legislative instruments (e.g. Cabinet Resolution No. (1) of 2025).

Rule III.E.2

VASPs must perform a risk-based assessment for every client using the criteria and methodology defined under Rules III.D.6 and III.D.7 (as discussed above).

Impact

Based on this risk based assessment, VASPs are required to assign a risk rating for each client that accurately reflects their AML/CFT risk profile.

Rule III.F

"Suspicious Transaction Report (STR)" has been replaced with the defined term *"AML-CFT Report"*. The new term encompasses all reports required by the UAE FIU, including STRs, Suspicious Activity Report (SAR), High-Risk Country reports, Funds Freeze Reports, and Partial Name Match Reports.

Impact

This marks a significant broadening of reporting obligations under the regulatory framework. This change ensures that VASPs are explicitly required to comply with the full suite of federal AML/CFT reporting duties, not just those limited to suspicious transactions. By adopting a defined, comprehensive term, VARA enhances regulatory clarity, aligns with federal expectations, and mitigates interpretive gaps. Operationally, VASPs must now ensure their systems and controls are capable of detecting, documenting, and filing all relevant *"AML/CFT Report"* types.

Compliance & Risk Management Rulebook - Changes and Impact

Rule IV.11-12 AND Rule V.B.6-7

The amendment prohibits VASPs from taking ownership of Client Money and Client VAs under any Client Agreement.

However, a narrow exception permits ownership only for the purpose of establishing a trust, where the VASP is the founder and clients are beneficiaries.

This transfer must fully comply with all provisions of the Client Money Rules and Client VA Rules accordingly, with continuous adherence required.

In case of Client VAs, the transfer of ownership to the trust must occur within one calendar day of receiving the VAs.

Impact

This effectively discontinues the 'title transfer regime', where legal ownership of client funds could be transferred to the service provider, often for collateral or operational purposes.

This shift reflects a deliberate policy choice to protect client funds from creditor claims, misuse, or commingling, particularly in insolvency scenarios.

The change closes a key legal loophole, preventing the recharacterisation of client funds (both money and VAs) as VASP assets and enhancing insolvency protection and fiduciary safeguards.

Rule V.B.3

VASPs must now clearly label all wallets always holding client VAs as 'Client VA Wallet' in their books and records.

Impact

This is a minor amendment intended solely to facilitate easier reference in the VASP's books and records, particularly for audit and regulatory supervision purposes.

Compliance & Risk Management Rulebook - Changes and Impact

Rule VII

This new section establishes the “*Sponsored Virtual Asset Service Provider (VASP) regime*” that permits unlicensed VASPs to operate under the umbrella of approved ‘Regulated Sponsors’, who bear full legal and regulatory accountability.

How to become a Regulated Sponsor?

To act as a Regulated Sponsor, a VASP must:

- (i) submit an application to obtain VARA’s approval. This application must demonstrate the Sponsor’s ability to meet ongoing compliance obligations and effectively supervise all Sponsored VASPs under its umbrella. VARA reserves the right to amend the application process at its discretion;
- (ii) meet the capital and prudential requirements of the Company Rulebook for each Sponsored VASP. The Regulated Sponsor may establish certain accounts on behalf of Sponsored VASPs (including Client Money Accounts and operating accounts), provided that all accounts remain segregated, are titled correctly, and maintain clear audit trails; and
- (iii) demonstrate that it has sufficient resources, expertise, and staffing to manage all relationships effectively, even in the event of business changes or expansions by a Sponsored VASP.

How to become a Sponsored VASP?

A Sponsored VASP must:

- (i) be a legal entity registered in Dubai; and
- (ii) receive prior approval from VARA before commencing any operations; and
- (iii) have the Regulated Sponsor as the controlling entity; or
- (iii) have the same controlling entity as the Regulated Sponsor.

The following additional conditions must be satisfied to be deemed as a Sponsored VASP:

- (i) Mandatory due diligence is required prior to onboarding wherein the Sponsors must ensure that the Sponsored VASPs are financially sound, operationally competent, and suitable to perform the proposed VA Activities.
- (ii) A written agreement must be executed between both parties, detailing the scope of permitted activities, compliance responsibilities, audit rights, termination provisions, and periodic reporting requirements.
- (iii) A full-time Responsible Officer who is approved by VARA and meets the criteria outlined in the Company Rulebook must be appointed by the Sponsored VASP.

Compliance & Risk Management Rulebook - Changes and Impact

Liability, Compliance and Oversight Responsibilities of the Regulated Sponsors

Regulated Sponsors face enhanced exposure, including for:

- (i) regulatory breaches committed by Sponsored VASPs;
- (ii) failures in governance, due diligence, or public disclosure; and
- (iii) inadequate control over onboarding, reporting, or data management.

Impact

The Sponsored VASP regime permits market entry through a controlled and supervised structure, placing full regulatory responsibility on the Regulated Sponsor.

It is a strategic regulatory innovation that broadens access to Dubai's virtual asset market while maintaining a high standard of compliance through centralised accountability.

Further, Regulated Sponsor must ensure the following:

- (i) the Sponsored VASPs are in compliance with all applicable Regulations, Rules, Directives, and all compulsory and the activity specific VARA Rulebooks.
- (ii) the Responsible Officer appointed by the Sponsored VASP remains continuously valid annually. In the event of any changes, the Regulated Sponsor must notify VARA in advance (or immediately in exceptional cases).
- (iii) All Personal Data collected by Sponsored VASPs remains segregated from their own systems and those of other Sponsored VASPs, in accordance with the Technology and Information Rulebook.
- (iv) In terms of reporting requirements, Sponsors must:
 - (a) oversee and report annually on complaints data, audited financials, and any other information requested by VARA.
 - (b) ensure that each Sponsored VASP maintains a separate Complaints handling procedure aligned with Market Conduct Rulebook requirements

Compliance & Risk Management Rulebook - Changes and Impact

Clarity regarding Regulatory Status

Sponsored VASPs may not present themselves as VARA-licensed VASPs. However, they are treated as deemed to be authorised for regulatory purposes, specifically for the VA Activities approved by VARA under the sponsorship model.

Marketing Communications by Sponsored VASPs

In all marketing and public disclosures, Sponsored VASPs must include:

- (i) the name and licence number of their Regulated Sponsor;
- (ii) clearly indicate their status as a Sponsored VASP; and
- (iii) publicly disclose their regulatory details, scope of authorised activities, any limitations, and the identity of their appointed Responsible Officer, in a machine-readable format on their website.

Impact

The Sponsored VASP regime also introduces:

(i) **Potential anti-competitive considerations:** By requiring the Regulated Sponsor and Sponsored VASP to share the same controlling entity, the framework risks favouring vertically integrated groups and excluding independent partnerships. This may concentrate market access in the hands of already-established players, raising barriers for standalone firms seeking sponsorship from unaffiliated VASPs.

However, VARA's discretionary power to refuse or terminate sponsorships based on perceived anti-competitive effects is a welcome safeguard. Accordingly, Sponsors with dominant market positions must be cautious to avoid exclusive arrangements or discriminatory sponsorship terms that could be construed as abuse of dominance or foreclosure under UAE competition principles.

(ii) **Heightened perception risk for Sponsors:** While the regulatory status of a Sponsored VASP is distinct and VARA has issued guidance requiring clear disclosures in marketing and public communications to reflect this, perception risks remain. These risks are particularly acute in situations where the distinction between VARA licensed VASPs and Sponsored VASPs with deemed authorisation becomes blurry. In such cases, the reputational consequences of any failure by a Sponsored VASP may disproportionately impact the Sponsor, regardless of the actual regulatory or factual circumstances.

(iii) **Governance complexity:** The Regulated Sponsor's obligations under this new regime are substantial. Therefore, there is an increase in the Sponsor's compliance and operational overhead, reinforcing the need for well-resourced compliance teams, scalable reporting systems, and proactive governance audits.

For the model to succeed, continued clarity from VARA on sponsorship eligibility, transparency in competition safeguards, and rigorous oversight of sponsor responsibilities is crucial.

Compliance & Risk Management Rulebook - Changes and Impact

Rule III.G

The amendment clarifies that VASPs must comply with all applicable Federal AML/CFT laws, including the Travel Rule obligations prescribed under UAE federal law. It is explicitly designated as a minimum baseline. Compliance with it does not exempt a VASP from adhering to broader or more stringent federal requirements.

VASPs are expressly required to report on their Travel Rule compliance in line with federal law and must be prepared to satisfy any additional procedural or reporting obligations imposed by VARA.

Impact

This amendment formalises a dual compliance regime, reinforcing that VASPs must align their operations with both VARA's regulatory framework and the UAE's overarching national AML/CFT legislation.

Rule III.J

VARA may now take enforcement action not only against the VASP entity, but also directly against its directors, Responsible Individuals (RIs), MLRO, and Senior Management for failures to comply with AML/CFT obligations.

Directors and key personnel must now demonstrate active engagement with AML/CFT governance, ensuring proper supervision and documentation are in place. The MLRO role is particularly exposed, reinforcing the need for operational independence, senior access, and adequate resourcing for individuals taking on these roles in VARA-licensed VASPs.

Impact

This marks a clear shift toward personal accountability and liability. This amendment raises the stakes for compliance personnel and compels VASPs to strengthen internal controls and clearly assign responsibilities to mitigate individual enforcement risk.

Compliance & Risk Management Rulebook - Changes and Impact

Rule III.E.10

A new provision mandates the application of Enhanced Customer Due Diligence (EDD) where:

- (i) a client is assessed as high-risk under Rules III.D.6 and III.D.7,
- or
- (ii) the client's Ultimate Beneficial Owner (UBO) is a Politically Exposed Person (PEP).

Impact

This removes discretion in tailoring the scope of EDD based on internal risk tolerance and obliges VASPs to fully integrate each measure into both onboarding and ongoing monitoring processes for high-risk clients.

In such cases, VASPs are required to implement additional measures, including:

- Collection of further identification data for the client and UBOs;
- Verification of the source of funds and source of wealth;
- More frequent updates to CDD information;
- Heightened transaction monitoring;
- Senior Management approval prior to onboarding;
- Requiring the first transaction to be routed through a regulated financial institution in a FATF-compliant jurisdiction;
- Verification of the natural person's current residential address (excluding P.O. boxes)

These obligations are to be embedded in both the onboarding and ongoing monitoring processes for high-risk clients. Importantly, the use of the conjunction "and" before the final requirement indicates that all listed measures must be applied cumulatively, rather than selectively.

Compliance & Risk Management Rulebook - Changes and Impact

Rule III.H

The revised regulations introduce a comprehensive and prescriptive Targeted Financial Sanctions (TFS) compliance regime for VASPs.

Impact

This amendment imposes substantial compliance burdens. It raises the threshold for operational readiness and reinforces a shift toward institutional-grade compliance in the virtual asset sector.

The new compliance regime for VASP's include:

- (i) Screening Requirements: VASPs must implement automated, real-time screening systems to detect clients and transactions involving designated entities under UNSC sanctions and Federal AML-CFT laws, with systems updated regularly. This introduces both technical and resource-intensive compliance expectations.
- (ii) Asset Freezing: VASPs are required to immediately freeze assets, including virtual assets and fiat, upon detecting a sanctioned party, and prevent any movement or access during the freeze. There is no discretion or grace period, demanding swift internal escalation and enforcement mechanisms.
- (iii) Record-Keeping: VASPs must retain comprehensive records of freezing actions and related transactions for a minimum of eight years, necessitating robust documentation and audit systems.
- (iv) Prohibition and Evasion Monitoring: All transactions involving sanctioned persons must be blocked, and VASPs must also detect and prevent circumvention attempts, requiring enhanced monitoring tools and staff training.
- (v) Policy and Governance Requirements: VASPs must establish formal TFS policies, with clear protocols for detection, escalation, enforcement, and regulatory reporting.