AZB & PARTNERS
ADVOCATES & SOLICITORS

Update – AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets, 2026

The Financial Intelligence Unit, Ministry of Finance, Government of India ("**FIU-IND**") has issued the updated "AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets" on January 08, 2026 ("**2026 Guidelines**") effectively replacing the erstwhile AML & CFT Guidelines issued on March 10, 2023 ("**2023 Guidelines**").

While the 2026 Guidelines for the most part, retain the broad AML/CFT architecture set out under the 2023 Guidelines, they consolidate the operational requirements earlier prescribed through multiple circulars and guidance documents issued by the FIU-IND from time to time, most notably the 'Circular for Registration of Virtual Digital Asset Service Providers (VDA SPs) in FIU India as Reporting Entity (RE)' dated September 15, 2025 ("**2025 Registration Circular**"), and the 'Guidance for Principal Officer (PO) – Minimum Requirements and Qualifications' dated February 25, 2025 ("**PO Guidance**"), which was not available in the public domain.

In effect, FIU-IND has now streamlined this AML/CFT framework into a single guidance document, consolidating multiple requirements (which were earlier scattered and/or not publicly accessible) to be adhered by Virtual Digital Asset Service Provider reporting entities ("**VDASP REs**").

We have captured the key highlights and changes in the 2026 Guidelines below:

1. FIU Registration Framework consolidated into the 2026 Guidelines.

1.1. One of the key features of the 2026 Guidelines is that they substantively incorporate and codify the end-to-end registration framework for VDASPs that was earlier set out through FIU-IND's 2025 Registration Circular.

1.2. Specifically, the 2026 Guidelines now contain a dedicated chapter titled "*Registration of VDASPs with FIU-IND*",[1] which absorbs and streamlines the procedural requirements introduced under the 2025 Registration Circular, covering the FINGate-based initiation of registration, issuance of temporary reference IDs, detailed document/information submissions, operational readiness checks, and the mandatory in-person meeting with live demonstrations of AML/CFT systems amongst others.

2. Minimum requirements and qualifications of a PO.

2.1. The 2026 Guidelines now specifically incorporate the minimum eligibility requirements for appointment of a Principal Officer ("**PO**"), which were set out under the PO Guidance, including, the following: -

(a) The PO must be a sufficiently senior officer at the management level at the VDASP RE who is exclusively responsible for ensuring adherence with the requirements under Chapter IV of Prevention of Money Laundering Act, 2002 and not be actively involved in other business or operational activities of the VDASP RE.

(b) The PO must be exclusively engaged with the VDASP RE on a full-time basis and cannot concurrently be engaged with another entity.

---

[1] Chapter 2 of the 2026 Guidelines.

(c) The PO should be thoroughly knowledgeable about legal issues surrounding the Anti-Money Laundering ("**AML**") framework, PMLA, AML/Terror Financing ("**TF**") risks and vulnerabilities, etc. and must have at least three (3) years of experience relating to this skill set.

(d) The PO should be permanently involved in high level decisions, which evaluate the ML/TF risks associated with products, services, delivery channels etc. and must have sufficient resources and support staff to effectively carry out implementation of the AML/TF program of the VDASP RE.

(e) The PO should enforce timelines and compliances relating to AML/TF as well as requests made by the FIU-IND. The PO should also frequently review AML/TF functions and place the same before the Board of Directors ("**Board**") / sub-committee of the VDASP RE preferably on a quarterly basis, etc.[2]

2.2. While the erstwhile PO Guidance stated that the "*PO should be preferably based out of India…*", the 2026 Guidelines now expressly require that the "*PO should be based in India…*". This change materially tightens the compliance position and is particularly relevant for multi-jurisdictional entities, where senior management and compliance personnel may be distributed across multiple locations (including outside India). Such entities may need to reassess their PO appointment and reporting structures to ensure alignment with the aforesaid revised requirement under the 2026 Guidelines.

3. Clear delineation of roles and responsibilities – DD & PO

3.1. The erstwhile 2023 Guidelines collectively captured the roles, responsibilities and obligations of a Designated Director ("**DD**") and a Principal Officer ("**PO**") in establishing effective mechanisms for combating money laundering, countering terrorist financing, and combating proliferation financing.[3] However, now the 2026 Guidelines clearly differentiate between the roles, responsibilities and obligations of a DD[4] and the PO.[5]

3.2. Responsibilities of the DD: The 2026 Guidelines further clarify the functions of the DD as a person responsible for ensuring the overall compliance of the VDASP RE with the AML / TF obligations prescribed under Chapter IV of the PMLA. Additionally, certain new responsibilities / obligations have been expressly identified for the DD under the 2026 Guidelines, as below:

(a) Evolve internal mechanisms for adherence to the procedure and manner of maintaining information as prescribed by the FIU-IND from time to time including proper upkeep of Customer Due Diligence ("**CDD**") records, transaction records and other related documents;

(b) Evolve an internal mechanism in adherence with the procedure and manner for furnishing information to FIU-IND as prescribed under Rule 7 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("**PMLR**"); and

---

2 Now captured under Paragraph 3.2 of the 2026 Guidelines.
3 Paragraph 5.4.2 of the 2023 Guidelines.
4 Paragraph 3.1 of the 2026 Guidelines.
5 Paragraph 3.3 of the 2026 Guidelines.

(c) Be responsible for carrying out risk assessment identify, assess and take effective measures to mitigate AML/TF risks with respect to clients, products, services, transactions etc.

3.3. Responsibilities of the PO: The 2026 Guidelines introduce a few additional and more granular implementation related responsibilities and obligations for the PO, as set out below:

(a) Analysis and decision-making in relation to the alert governance framework, including verification and retention of relevant records and documents for audit purposes;

(b) Recording of reasons for treating any transaction / series of transactions as suspicious transactions and ensuring that there is no undue delay in determining such transactions as suspicious;

(c) Decision making in relation to non-reportability of certain alerted transactions and recording the reasons for such decisions;

(d) Periodic review of the list of alerted transactions and the reporting mechanisms in the VDASP RE to ensure continued compliance. This will also include conducting surprise checks of the data being monitored by the AML compliance team of the VDASP RE to avoid / mitigate any gap.[6]

3.4. Additionally, the 2026 Guidelines also require the PO to report the following matters to the Board or a designed sub-committee (if any) on an annual basis:

(a) Assessment of the effectiveness of the AML/TF program of the VDASP RE and identification of any risks or vulnerabilities thereof;

(b) Summary of suspicious transaction reports and other reports prescribed under the PMLA and PMLR;

(c) Proposed changes to the AML/TF policy of the VDASP RE;

(d) Any instructions, red-flag indicators, guidance etc. issued by the FIU-IND from time to time; etc.

4. Risk Classification Identified.

4.1. The 2026 Guidelines strengthen internal control and oversight by requiring a more standardised and governance-driven approach towards risk assessment and client risk classification.

4.2. Under the revised framework, risk assessments must be formally documented, proportionate and subject to Board-driven periodicity, with an express safeguard that the interval between two risk assessments must not exceed one year.[7]

4.3. Importantly, client risk classification is now expressly required to be conducted through a Board-approved framework which, at a minimum, categorises clients into High Risk and Medium Risk buckets (with flexibility to create additional categories as necessary). The Guidelines further mandate a periodic review of such client risk classification at least once every six months.[8]

---

6 Paragraph 3.3 of 2026 Guidelines.
7 Paragraph 3.6.1(d) of 2026 Guidelines.
8 Paragraphs 3.6.2(a) and 3.6.2(c) of 2026 Guidelines.

5. CDD Requirements Tightened.

5.1. The 2026 Guidelines introduce a material tightening of the CDD framework, reflecting a shift from a largely principle-based approach in the 2023 regime to a far more implementation specific regime.

5.2. Chapter 4 of the 2026 Guidelines now prescribes a significantly enhanced CDD dataset and control environment, including the capture of additional technical identifiers such as IP address (with timestamp), geo-location, device IDs, wallet addresses and transaction hashes, etc.[9]

5.3. The 2026 Guidelines further mandate specific onboarding safeguards aimed at mitigating impersonation and synthetic identity risks such as:

(a) Obtaining a selfie with liveness detection and capturing latitude/longitude of onboarding location with timestamp and IP address,[10]

(b) Verification of the mobile number and email id of the client through OTP validation or link-based verification methods;[11]

(c) Requiring live photo-based verification with liveness detection,[12]

(d) Treating mismatch between address and geo-coordinates as a trigger for enhanced measures;[13]

(e) Verification of the client's bank account through a penny-drop mechanism.[14]

5.4. The periodic CDD updation framework has also been tightened by introducing more specific minimum timelines, i.e., half yearly updates for clients that are assessed as high-risk, and annual updates for other clients.[15]

6. Audit & Board Oversight Strengthened.

6.1. While the requirement for independent review of AML controls existed in the earlier framework under the 2023 Guidelines, the 2026 Guidelines place greater emphasis on audit robustness and requirement to place the audit report before the Board / designated sub-committee (if any).

6.2. Further, the 2026 Guidelines now expressly provide that reporting entities should cause an independent audit of AML/CFT/CPF controls, systems, procedures and safeguards, on an annual basis, with corrective actions required for identified deficiencies.[16]

---

9 Paragraph 4.1.4(b) of 2026 Guidelines.
10 Paragraph 4.2.1 of 2026 Guidelines.
11 Paragraph 4.2.3 of the 2026 Guidelines.
12 Paragraph 4.2.4 of 2026 Guidelines.
13 Paragraph 4.2.5 of 2026 Guidelines.
14 Paragraph 4.2.6 of 2026 Guidelines.
15 Paragraph 4.5.2 of 2026 Guidelines.
16 Paragraph 3.6.3 of 2026 Guidelines.

7. Implementation-Focused Chapter 5.

7.1. Chapter 5 of the 2026 Guidelines represents a meaningful shift towards implementation-oriented compliance, with multiple provisions prescribing concrete systems expectations and operational controls:

(a) The transaction monitoring framework is expanded to include more explicit design expectations, including the requirement that monitoring systems should be capable of identifying the origin and destination of a VDA and detect potential ML/TF/PF activities.[17]

(b) Reporting entities are also encouraged to adopt transaction risk scoring models and may consider use of AI technologies to support monitoring.[18]

(c) Systems are required to be scalable and secure to enable storage of transaction data such that individual transactions can be reconstructed, with role-based access controls and robust backup/recovery mechanisms.[19]

(d) The Travel Rule is significantly operationalised, including requirements to deploy appropriate technological solutions to support real-time secure transmission of originator/beneficiary information and an express clarification that post-facto submission is not permitted.[20]

(e) Additionally, the VDASP REs are required to submit a report to the FIU-IND on a monthly basis that will include essential metrics, activity indicators, compliance status etc. and any other details as prescribed by the FIU-IND from time to time.[21]

7.2. Overall, Chapter 5 functions as a compliance implementation blueprint, signalling FIU-IND's expectation for demonstrable technical capability, monitoring sophistication and auditable control environments.

8. Recordkeeping Requirements Tightened.

8.1. Although the record retention framework under the PMLA/PMLR remains broadly consistent, the 2026 Guidelines introduce a key operational tightening by expressly requiring reporting entities to preserve complete audit trails in a tamper-proof manner.

8.2. The 2026 Guidelines specifically require preservation of audit trails including verification responses, timestamps and authentication logs, which indicates FIU-IND's expectation for stronger evidentiary integrity, forensic traceability and system-level accountability.[22] In practice, this may require strengthening database logging controls, access logging and immutability standards (including for KYC verification events), and would also be directly relevant for regulatory reviews, audits and information requests under the PMLA framework.

---

17 Paragraph 5.2.1 of 2026 Guidelines.
18 Paragraph 5.2.4 of 2026 Guidelines.
19 Paragraph 5.2.3 of 2026 Guidelines.
20 Paragraphs 5.3.3 and 5.3.4 of 2026 Guidelines.
21 Paragraph 5.7 of the 2026 Guidelines.
22 Paragraph 6.2(f) of 2026 Guidelines.

9. New Prohibited Categories of VDAs.

9.1. The 2026 Guidelines introduce certain brand-new risk stances and prohibitions under the "Other Measures" Chapter,[23] reflecting a tightening of FIU-IND's acceptable risk appetite for high-anonymity VDA products/services. In this regard, it is pertinent to note the following:

(a) The FIU-IND has expressly discouraged Initial Coin Offerings (ICOs) / Initial Token Offerings (ITO) owing to its inherently elevated risks and potential misuse;[24]

(b) With respect to VDA transactions involving unhosted wallets, VDASP REs are required to collect data on such unhosted wallet transfers, monitor and assess the information necessary to determine the risk associated with such transactions, and apply appropriate EDD measures and other risk-based controls.[25]

9.2. Notably, the Guidelines now set out a framework for dealing with unregistered VDASPs and reiterate that obligations under the FIU regime are activity-based and apply regardless of physical presence in India and further contemplate compliance exposure including potential action under Section 13 of PMLA for non-registration.[26]

9.3. More prominently, the Guidelines introduce a clear prohibition-style stance against Anonymity-Enhancing Crypto Tokens (AECs) and similar VDAs designed to conceal or obfuscate origin/ownership/value, treating such activity as unacceptably high risk and outside permissible risk appetite.[27]

9.4. A similar non-facilitation approach is introduced for transactions involving crypto tumblers/mixers and other anonymity-enhancing products/services, requiring monitoring and analytical tools to detect such activity and a clear expectation that such transactions should not be facilitated.[28]

To summarize, the 2026 Guidelines reflect FIU-IND's clear pivot towards operational verification and implementation, particularly around registration diligence, governance accountability (DD/PO), tightened CDD controls, structured client risk classification, and technology-driven monitoring/travel rule compliance. This consolidated framework also reduces interpretational gaps by pulling multiple circular/guidance-based expectations into a single streamlined guideline document.

****

23 Chapter 7 of 2026 Guidelines.
24 Paragraph 7.1.3 of the 2026 Guidelines.
25 Paragraph 7.2.2 of the 2026 Guidelines.
26 Paragraph 7.3 of 2026 Guidelines.
27 Paragraph 7.4 of 2026 Guidelines.
28 Paragraph 7.5 of 2026 Guidelines.