Virtual Assets

Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

July 2026

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2026), *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France*,
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

Table of Contents

Executive Summary

1. This targeted update assesses progress and remaining gaps in the implementation of Recommendation 15 (R.15) across the FATF Global Network, following the extension of the FATF's AML/CFT Standards to virtual assets (VAs) and virtual asset service providers (VASPs). In line with the FATF Virtual Assets Contact Group (VACG) Roadmap to strengthen implementation of R.15, the report provides an updated overview of measures taken by FATF and FSRB jurisdictions, including jurisdictions with materially important VASP activity, to regulate and supervise the VA/VASP sector.
2. Since the 2025 Targeted Update, jurisdictions have continued to make progress in implementing R.15, including by conducting VA/VASP risk assessments, developing regulatory approaches, licensing or registering VASPs, implementing the Travel Rule, and advancing supervisory and enforcement action. However, significant gaps remain in translating risk assessments into effective mitigation measures, operationalising licensing or registration frameworks in practice, identifying persons or entities conducting VASP activities, and ensuring effective risk-based supervision and enforcement.
3. The report also highlights emerging and increasing risks involving VAs, including the growing industrialisation of VA-enabled fraud by organised crime groups, the misuse of stablecoins, risks arising from P2P transactions through unhosted wallets, offshore VASPs operating outside effective regulatory and supervisory oversight, and continuing challenges related to DeFi arrangements. In response, the report sets out recommendations for the public and private sectors to strengthen R.15 implementation, improve risk mitigation, and enhance domestic, international, and public-private co-operation.

Key Findings

- Overall, there has been some improvement in the implementation of R.15 since 2025. More jurisdictions reported having conducted VA/VASP risk assessments, but effectively using these assessments to inform risk-based preventive, mitigation, supervisory and enforcement measures continues to be a challenge for many jurisdictions.
- Jurisdictions are increasingly determining how to regulate their VA/VASP sector, but significant gaps remain. More jurisdictions have identified their regulatory approach, including by permitting VA/VASP activity or adopting full or partial prohibitions. However, further analysis is needed to understand the extent to which these frameworks have been effectively operationalised.
- Jurisdictions taking a prohibition approach have not progressed in taking supervisory or enforcement actions to sanction VASPs operating illegally within their jurisdictions. The use of prohibition frameworks, while allowed by the FATF Standards, can represent significant risks to the VASP and global financial system if not enforced effectively.
- Progress has continued in licensing and registering VASPs, including in supervisory inspections and enforcement actions. Nevertheless, further progress is needed in licensing and registration in practice, and jurisdictions continue to face difficulties in identifying natural or legal persons that conduct VASP activities. Offshore VASPs also remain a significant challenge, with more than a third of jurisdictions with licensing or

registration frameworks applying a broader approach to require certain offshore VASPs to be licensed or registered.

- Jurisdictions have made progress on implementing the Travel Rule. For the 2026 survey, 83% of respondents reported having passed legislation implementing the Travel Rule. However, enforcement experience remains limited, with almost half of jurisdictions that have introduced Travel Rule legislation not yet having taken Travel Rule-related supervisory or enforcement action.
- Similar to findings in previous Targeted Update reports, identifying individuals or entities exercising control or sufficient influence over DeFi arrangements continues to be challenging. While some jurisdictions (31% 44 of 142) reported that their risk mitigation measures apply to DeFi arrangements, only four jurisdictions have imposed licensing or registration requirements, and just two have actually licensed or registered such arrangements in practice.
- Since 2025, VA-enabled illicit activity has become more complex and convergent, including through Organised Crime Groups-linked scam centre operations, "pig-butchering" scams, DPRK-related cyber theft, TF/PF, sanctions evasion and cross-border money laundering. Stablecoins, P2P transactions through unhosted wallets, offshore VASPs, OTC brokers, cross-chain tools and DeFi-related activity continue to present significant risks, highlighting the need for stronger public-private cooperation, enhanced monitoring, and concrete risk mitigation measures by both jurisdictions and the private sector.

Recommendations for the public and private sectors

The following are priority recommendations for the implementation of R.15. Jurisdictions with materially important VASP activity should expedite the effective implementation of R.15. Those that have not yet implemented R.15 should start by prioritising risk assessments and setting up a legal framework. Jurisdictions that have already taken steps to implement R.15 should prioritise practical supervisory activity.

Recommendations for the Public Sector

Understand and comprehensively assess the ML/TF/PF risks posed by VAs and VASPs (even where choosing to prohibit VASPs)

1. Develop a clear and thorough understanding of the ML/TF/PF risks posed by VAs and VASPs in order to allocate supervisory and enforcement resources proportionate to the national risk and context. The risk assessment of VAs and VASPs should consider the jurisdiction's overall exposure (materiality) as well as the specific ML/TF/PF risks associated with:

   i. VASPs established or created in the jurisdiction;
   ii. VASPs operating or offering services within the jurisdiction (oVASPs);
   iii. Stablecoin issuers and DeFi arrangements that have controllers based or operating in the jurisdiction;
   iv. Peer-to-peer transactions and unhosted wallets;

v. Emerging technologies, business models, trends and methods in the VA ecosystem.

2. Rely on a broad range of credible resources to conduct the VAs/VASPs risk assessment. While the FATF does not prescribe a specific methodology for assessing the VA/VASP sector, jurisdictions should be able to demonstrate that they have identified and understood the ML/TF/PF risks posed by VAs and VASPs and that they have implemented appropriate and effective mitigating measures.

Adopt a robust supervisory framework for VAs and VASPs

3. Prioritise efforts and allocate supervisory resources to identify and assess the ML/TF/PF risks associated with VAs and VASPs and implement an appropriate supervisory framework in line with Recommendation 15. This should include:

   i. *Licensing or registration requirements*: Imposing appropriate licensing or registration requirements on VASPs incorporated or established in the jurisdiction, including stablecoin issuers and qualifying DeFi arrangements that fall within the scope of the FATF Standards.[1] Where relevant, require VASPs operating cross-border (oVASPs) to be licensed or registered.
   ii. *Supervisory inspections and guidance*: Conducting both off-site and on-site inspections of VASPs and providing feedback and guidance on the effectiveness of their AML/CFT/CPF compliance frameworks, including the implementation of the Travel Rule.
   iii. *Enforcement against unlicensed activity*: Adopting effective measures to identify and sanction natural or legal persons that, in practice, conduct VASP activities without the required license or registration.

Enhance international and public-private cooperation to investigate and seize illicit assets

4. Substantially strengthen collaboration with foreign counterparts and relevant private-sector stakeholders to ensure that criminal activities linked to existing and emerging ML/TF/PF risks can be effectively disrupted in practice, whether these activities involve VASPs, peer-to-peer transactions, or unhosted wallets. This may be achieved by:

   i. *Establishing cooperation mechanisms*: Creating and utilising both formal and informal international and domestic cooperation channels to facilitate timely information sharing for the identification of illicit assets and threat actors.

   ii. *Enabling effective asset freezing and confiscation*: developing adequate operational infrastructure, legal frameworks, and protocols involving public authorities and private-sector partners to enable the rapid tracing, freezing and seizure of illicit virtual assets.

[1] The FATF distinguishes three broad categories of DeFi arrangements: (i) those with identifiable controllers ("centralised"); (ii) those that are centralised in practice but where controllers cannot be readily identified; and (iii) those that are truly decentralised. The FATF Standards apply to the first two categories. While truly decentralised arrangements fall outside the scope of the Standards, as the latter cannot be readily applied to them, such arrangements still present significant risks that require alternative, risk-based mitigation measures.

Recommendations for the Private Sector

5. VASPs, including Stablecoin issuers and qualifying DeFi arrangements, should establish robust AML/CFT/CPF compliance frameworks and implement the Travel Rule in line with the requirements of R.15. VASPs should ensure that:

    i. they thoroughly understand their institutional risk, and assess emerging risks associated with stablecoins, P2P transactions, unhosted wallets, oVASPs and DeFi-related activities.

    ii. their AML/CFT controls, including KYC, wallet screening, blacklisting, and, where appropriate, whitelisting mechanisms as well as freezing and blocking capabilities adequately mitigate identified risks and can be swiftly updated to respond to emerging ML/TF/PF trends and typologies.

    iii. They proactively collaborate with competent authorities and private sectors to identify, investigate and prosecute illicit activity by sharing typologies, red flags, good practices, and ensuring that they can provide tactical and operational assistance in the course of law enforcement investigations.

6. On the basis of the findings of the FATF Targeted Reports and related recommended actions, VASPs should:

    i. strengthen the monitoring of transactions involving unhosted wallets by applying enhanced due diligence measures for higher-risk wallet activity.

    ii. identify suspicious patterns in VA transactions and detect rapid transfer of VAs using transactions monitoring and blockchain analytics tools.

    iii. Conduct enhanced due diligence of oVASPs, detect accounts used by oVASPs that misrepresent themselves as retail users, restrict or exit higher-risk relationships, and monitor fiat on- and off-ramp activity linked to unlicensed or weakly supervised offshore platforms.

    iv. Assess risks arising from DeFi activities, including exposure to protocols, bridges, mixers, cross-chain tools, and apply appropriate AML/CFT/CPF measures to mitigate those risks.

Next steps

In February 2023, the FATF adopted a Roadmap to strengthen implementation of R.15. In line with the Roadmap, the FATF has updated the table that sets out the status of implementation of R.15 (e.g., undertaking a risk assessment, enacting legislation to regulate VASPs, conducting a supervisory inspection, etc.) by all FATF members and other jurisdictions with materially important VASP activity (MIVA table). The FATF has also published a number of Targeted Reports to provide further guidance to jurisdictions on key issues, including the implementation of the Travel Rule, risks related to offshore VASPs, and ML/TF/PF risks associated to Stablecoins and unhosted wallets via peer-to-peer transactions, and DeFi arrangements.

The Targeted Update Reports and the updated MIVA table consistently show modest year-on-year improvements in the implementation of Recommendation 15 across the FATF Global Network. Persistent challenges remain in the risk assessments, travel rule, regulation/supervision, and enforcement actions.

The FATF will continue to monitor the implementation of R.15 and emerging risks within the virtual assets ecosystem, with particular attention to jurisdictions with significant VASP sectors, and will use its existing toolkit, including assessment, risk analysis and capacity building, to enhance the global status of compliance.

Introduction

1. Following the October 2018 update to Recommendation 15 (R.15), which brought virtual assets (VAs) and virtual asset service providers (VASPs) within the scope of the FATF's AML/CFT requirements, and the June 2019 adoption of the Interpretive Note to R.15, the FATF has undertaken substantial work to address implementation gaps, provide guidance to jurisdictions to support effective implementation (see Table 1.1), and monitor evolving risks in the virtual asset sector.

Table 1.1. Overview of FATF work on VAs and VASPs

2018	• Recommendation 15 amended
2019	• Adoption of Interpretive Note to R.15 • Creation of the FATF Virtual Assets Contact Group (VACG) • Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021)
2020	• 12 month review of the new FATF Standards: 1st12-month review • Report to the G20: FATF Report to the G20 on So-called Stablecoins • Risk indicators: List of Red Flag Indicators of ML/TF through VAs
2021	• Updated guidance for regulators[2]: Updated Guidance for a Risk-Based Approach to VA and VASPs • 24 month review of the FATF Standards: 2nd12-month review
2022	• Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs
2023	• Report on ransomware, with a focus on VA risks and trends: Countering Ransomware Financing • Report on implementation of R.15: VAs: Targeted Update on Implementation of the FATF Standards
2024	• Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity
2025	• Targeted Update on Implementation of the FATF Standards on VAs and VASPs • Travel Rule Supervision – Best Practices
2026	• Targeted Report on Stablecoins and Unhosted Wallets (P2P transactions) • Understanding and Mitigating the Risks of Off-shore Virtual Asset Service Providers • Targeted Report on Regulatory Challenges from Decentralised Finance (DeFi) • Targeted Update on Implementation of the FATF Standards on VAs and VASPs

[2] The 2021 Guidance includes updates focusing on the following six key areas: clarification of the definitions of virtual assets and VASPs; guidance on how the FATF Standards apply to so-called stablecoins; additional guidance on the risks and the tools available to countries to address the ML/TF risks for peer-to-peer transactions; updated guidance on the licensing and registration of VASPs; additional guidance for the public

2. This report is the FATF's seventh update on the global implementation of its Standards for VAs and VASPs. It provides an overview of implementation of R.15, including the Travel Rule. The analysis focuses on technical requirements of the Standards, highlighting the extent to which jurisdictions have implemented the specific requirements of R.15, including legal and regulatory frameworks, enforceable measures, and the existence, powers, and procedures of competent authorities. It also outlines key challenges in implementing the FATF Standards for VAs and VASPs, highlights progress made by both the public and private sectors, and identifies emerging good practices. Finally, the report provides an overview of emerging risks relating to VAs, and jurisdictions and industry responses to these risks.

3. The analysis included in this report is based on:
   - A 2026 survey of jurisdictions' implementation of R.15, including the Travel Rule, and responses to emerging risks. The survey collected responses from 147 jurisdictions (38 FATF members and 109 FSRB members). Responses were self-reported and have not been independently verified. The survey applied conditional branching (skip logic), whereby respondents were directed to specific questions based on their responses to previous questions (e.g., respondents that had not yet decided whether to prohibit or regulate VASPs were not asked questions on Travel Rule implementation). As a result, the number of respondents to each question group varied.[3] For the purpose of this analysis, the report infers that jurisdictions (58 out of 205) that did not respond to the survey have not made progress on R.15, including Travel Rule implementation.[4]
   - VACG meetings (September 2025; May 2026) and the VACG symposium (December 2025).
   - Results from 149 completed and published FATF mutual evaluation reports (MERs) and follow-up reports (FURs) that assess R.15 (as of April 2026).

4. This report comprises the following sections:

   - **Section 1** provides an overview of jurisdictions' implementation of R.15 including the Travel Rule across the FATF's global network and considers major challenges faced in assessing ML/TF/PF risks, licensing or registering VASPs, and regulating offshore VASPs.
   - **Section 2** considers market developments and emerging risks, in particular the increasing use of stablecoins by criminals across all crime types and the use of VAs to launder the proceeds of predicate offences, particularly fraud and scams, fund terrorism and finance the proliferation of weapons of mass destruction.
   - **Section 3** sets out the next steps for the FATF and VACG.
   - **Annex A** provides updated table of FATF members and other jurisdictions from across the FATF global network with materially important VASP activity.

---

and private sectors on the implementation of the Travel Rule; and principles of information-sharing and co-operation amongst VASP supervisors.

3 Risk assessment and policy approach to VASPs: 145 respondents; licensing/registering and supervising VASPs: 130 respondents; Travel Rule implementation: 129 respondents; DeFi; 142 respondents; treatment of NFTs, unhosted wallets, and P2P: 138 respondents.

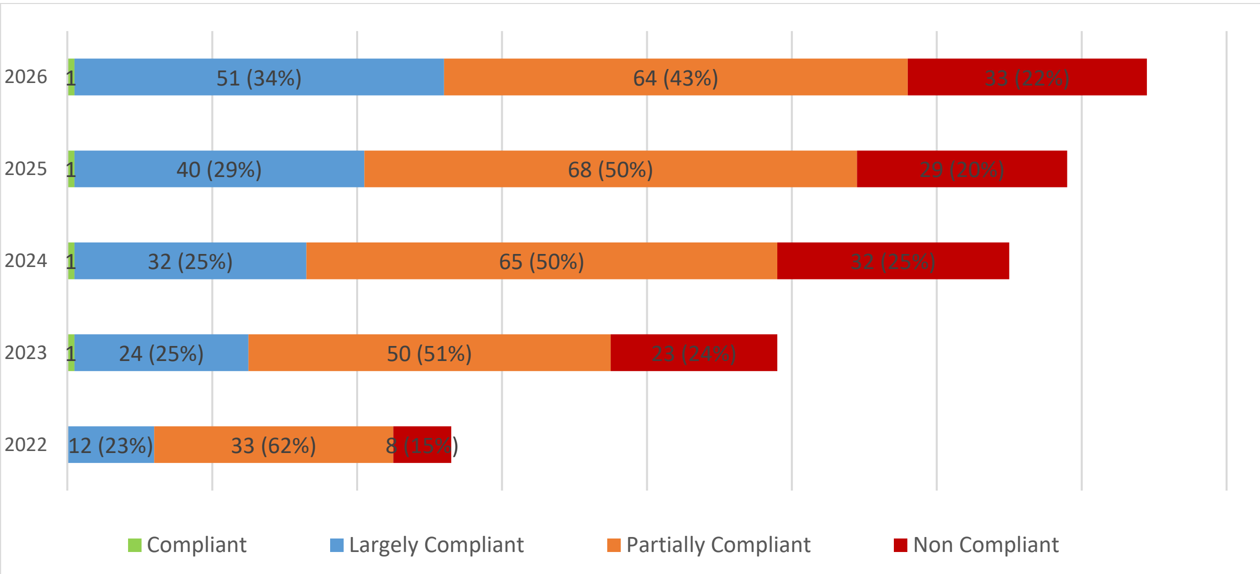
4 FATF and the Global Network consist of 205 jurisdictions in total. 147 jurisdictions responded to the 2026 survey.

SECTION ONE: Jurisdictions' Implementation of FATF Standards on VAs/VASPs (R.15)

2.2. Overall Status of R.15 Implementation in Mutual Evaluation and Follow-up Reports

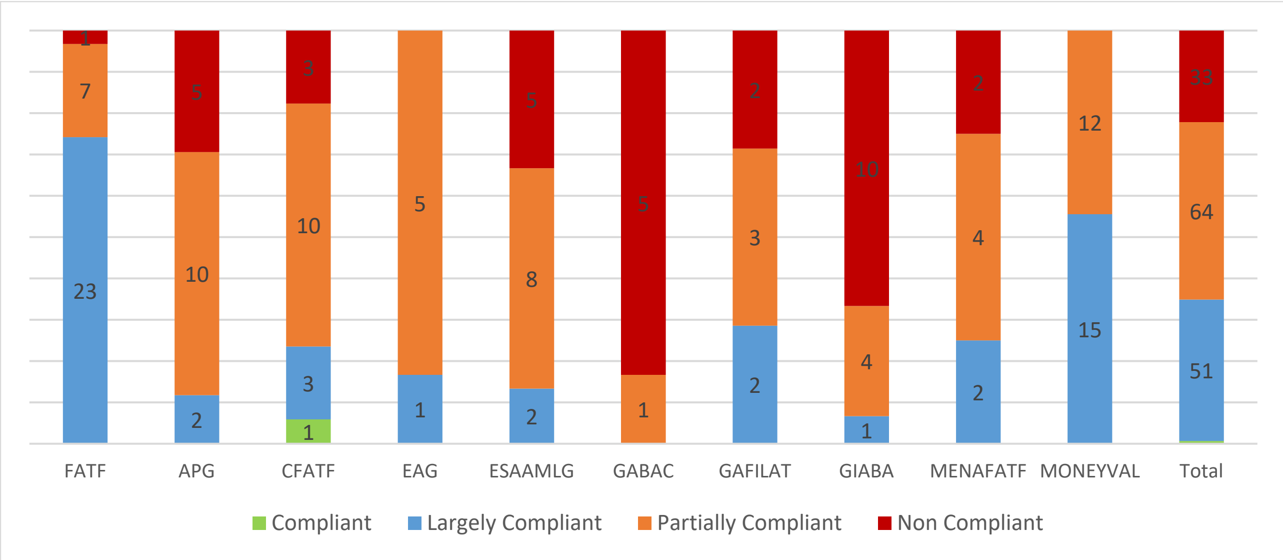
5. As of April 2026, 149 jurisdictions have been assessed for compliance with the FATF standards for VAs and VASPs. The data below reflect ratings related to technical compliance with the FATF requirements, as set out in R.15 and INR.15[5] (see Figure 1.1). Global implementation has slightly improved since 2025. The proportion of jurisdictions that are largely compliant (LC) increased from 29% (40 of 138 jurisdictions) in 2025 to 34% (51 of 149 jurisdictions) in 2026, and the proportion of jurisdictions partially compliant (PC) with the revised R.15 also decreased slightly from 50% (68 of 138 jurisdictions) in 2025 to 43% (64 of 149 jurisdictions) in 2026.
6. The proportion of jurisdictions not compliant (NC) with the requirements remains similar from 21% (29 of 138 jurisdictions in 2025) to 22% (33 of 149 jurisdictions in 2026). As in 2025, only one jurisdiction continues to be fully compliant (C) with R.15.
7. Implementation varies across regions (see Figure 1.2), with lower capacity jurisdictions struggling to implement R.15.

Figure 1.1. Assessment results: Compliance with R.15 (as of April 2026)



[5] Results of R.15 assessments have been analysed since the 2022 Targeted Update. These include Mutual Evaluations and Follow-up reports.

Figure 1.2. Assessment results: Compliance with R.15 by FATF/FSRB (as of April 2026)[6]



8. Compared to 2025, jurisdictions made positive progress in 2026 in implementing most requirements overall. However, many jurisdictions still face challenges in conducting risk assessments and implementing the Travel Rule (see Figure 1.3). The key gaps reflected in these assessment results, including challenges related to risk assessments, licensing or registration, supervision, and Travel Rule implementation, are addressed in subsequent sections.

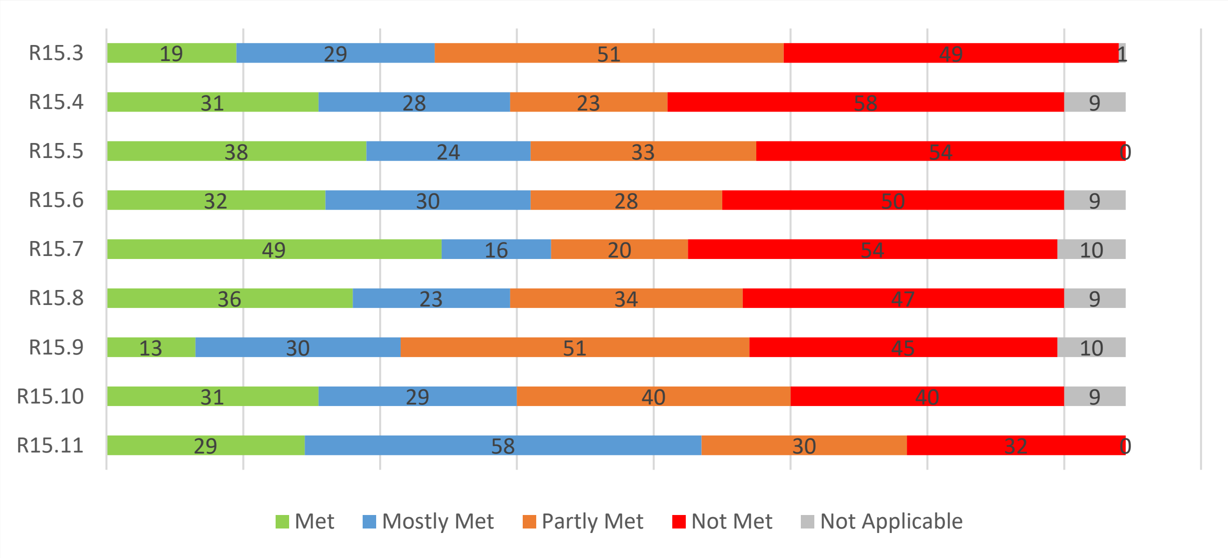
Table 1.2. FATF Assessment Methodology for requirements on VAs/VASPs

R15.3	Risk assessment and application of a risk-based approach
R15.4	Licensing/Registration of VASPs
R15.5	Identification of natural persons or legal entities that conduct VASP activities
R15.6	Supervision/Regulation of VASPs to ensure AML/CFT compliance
R15.7	Establishment of guidelines which assist VASPs in AML/CFT compliance
R15.8	Sanctions compliance
R15.9	Preventive AML/CFT measures including the Travel Rule
R15.10	Targeted Financial Sanctions compliance
R15.11	International cooperation

Source: FATF Methodology for assessing compliance with the FATF Recommendations, available at: www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html

[6] Joint FATF/FSRB members are only counted in the FATF column.

Figure 1.3. Assessment results: Compliance with individual R.15 criteria (as of April 2026)[7]

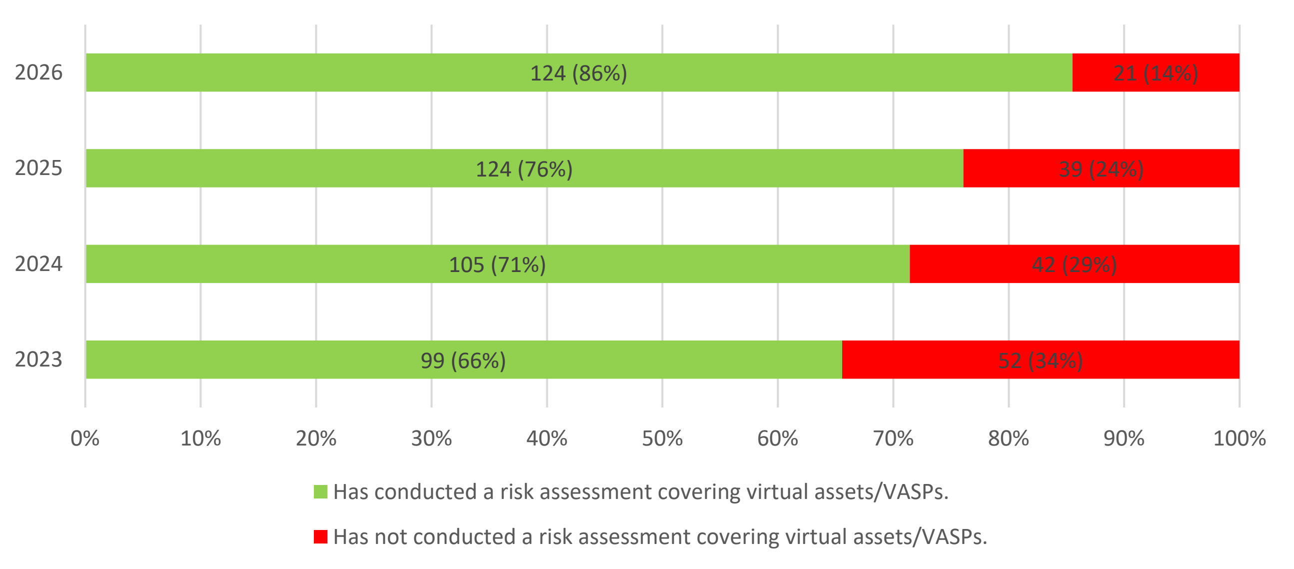


2.3. Challenges assessing ML/TF/PF risks of VAs and VASPs

9. The results of the FATF's 2026 survey show that the vast majority of respondents (86%; 124 of 145 jurisdictions) reported having conducted an ML/TF/PF risk assessment for VA/VASP risks (see Figure 1.4). This reflects an increase in the proportion of responding jurisdictions reporting that they had conducted such a risk assessment, from 76% in 2025 (124 of 163) to 86% in 2026.

[7] For details on R.15 criteria see FATF Methodology for assessing compliance with the FATF Recommendations

Figure 1.4. Survey results: Has your jurisdiction conducted a risk assessment of VAs/VASPs?



10. However, while many jurisdictions have conducted a risk assessment, challenges still remain in implementing preventive and/or mitigation measures in line with identified risks or using the results of the risk assessments to implement risk-based supervision. This is demonstrated by the findings from FATF mutual evaluations that show only 48 out of 149 assessed jurisdictions met or mostly met sub-criterion 15.3 on assessing risk and taking a risk-based approach (see Figure 1.3).
11. Jurisdictions are encouraged to refer to the FATF's 2021 Guidance, which includes factors to consider when undertaking a VA risk assessment and applying a risk-based approach. In addition, jurisdictions may consult the FATF's Community Workspace on Virtual Assets[8], which includes several examples of VA risk assessments, as well as materials from the December 2025 VACG symposium. The symposium covered a range of topics related to conducting risk assessments of VAs/VASPs, including developing methodologies and translating findings into action plans and/or national strategies. Jurisdictions are also encouraged to consult the FATF ML NRA Guidance[9], including any subsequent updates, which are expected to include a VA/VASP annex later in 2026.

2.4. Challenges developing, implementing and enforcing a regime for VASPs

2.4.1. Developing and implementing a regime for VASPs

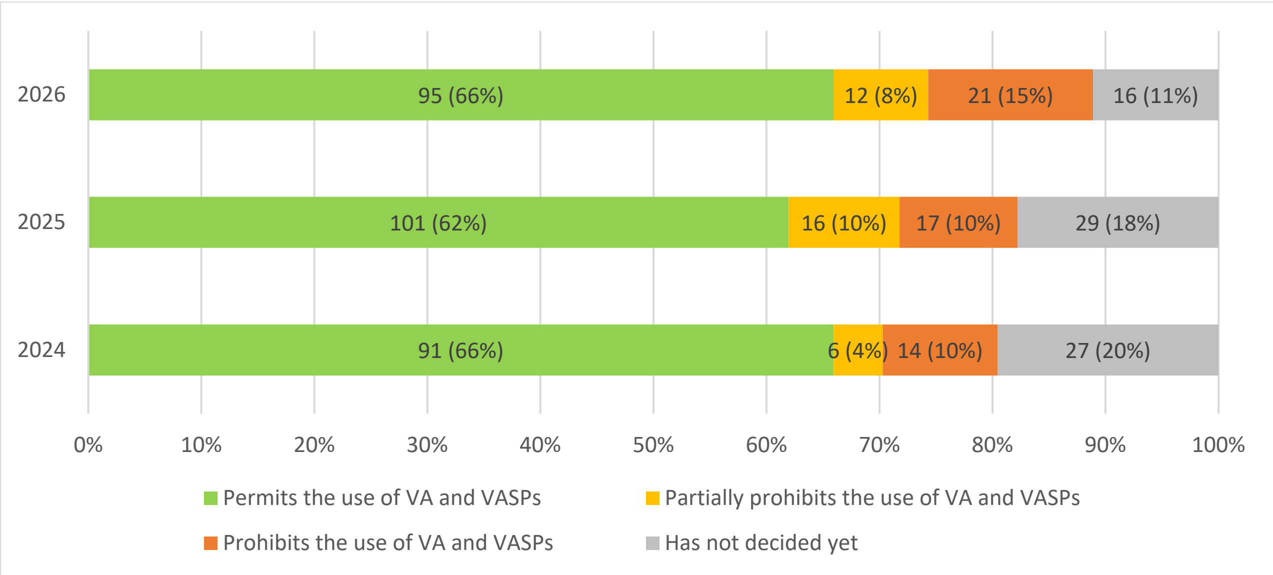
12. Notably, an increasing proportion of jurisdictions have identified how they intend to regulate the VA sector, increasing from 82% in 2025 (134 of 163 jurisdictions) to 89% (128 of 144 jurisdictions) in 2026 (see Figure 1.5). However, a minority of jurisdictions continue to report that they have not yet decided if and how to regulate the sector. This proportion decreased from 2025 (18%; 29 of 163 jurisdictions had not decided on their approach) to 2026 (11%; 16 of 144 jurisdictions). Most

[8] FATF Virtual Assets - Home

[9] https:www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Guidance.html; and https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Toolkit-Annexes.html

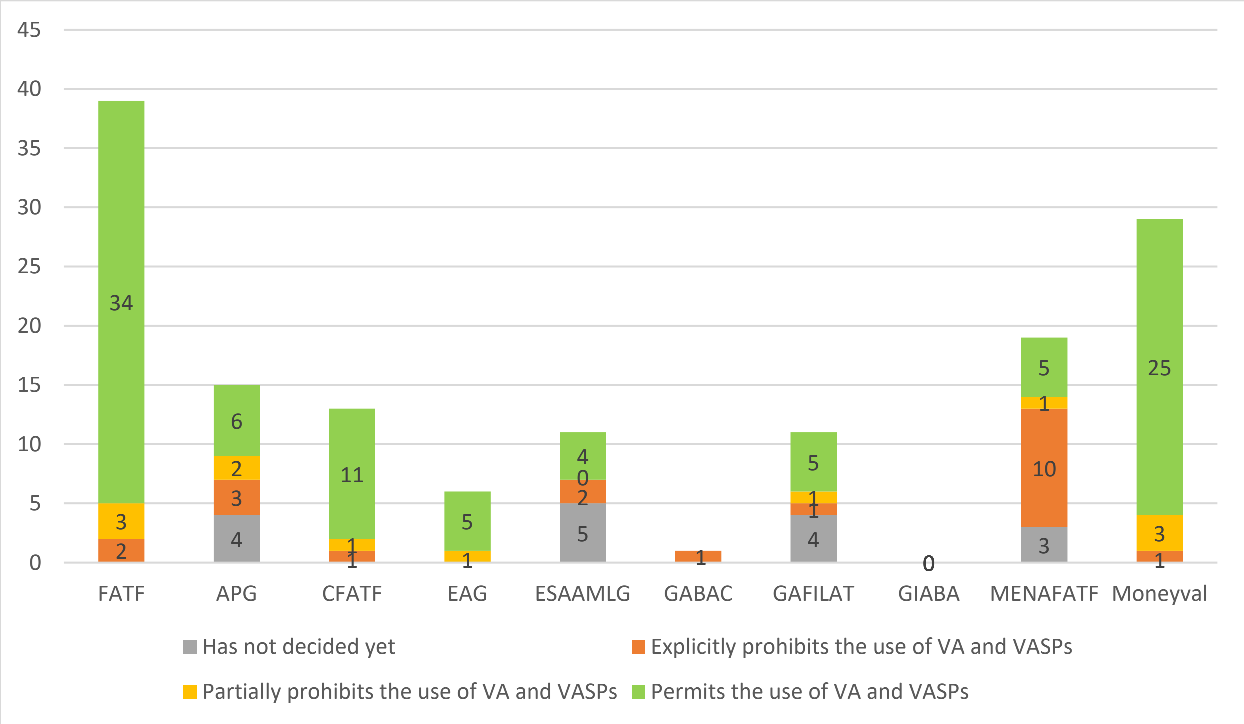
jurisdictions (66%; 95 of 144 respondents) have decided to permit the use of VAs and the operation of VASPs. In contrast, 23% of respondents reported opting to prohibit VASPs, indicating a steady increase over the past few years, rising from 11% of survey respondents in 2023 (16 of 151), 14% in 2024 (20 of 147) and 20% in 2025 (33 of 163). While a prohibition is permissible under the FATF Standards, as discussed in previous Targeted Updates, it may be difficult to implement effectively unless jurisdictions take proactive steps to identify prohibited VA/VASP activities and apply appropriate supervisory and enforcement measures to prevent and sanction such activities. An increase in the use of prohibitions may therefore raise concerns in the future if jurisdictions are not able to enforce them effectively.

Figure 1.5. Survey results: What is your jurisdiction's approach to VAs and VASPs?



13. A prohibition approach appears to be more common in certain regions. Similar to the results in the 2025 report, survey responses show that members of MENAFATF (Middle East and North Africa region) have more commonly chosen a partial or total prohibition approach compared to members of other FSRBs (see Figure 1.6).

Figure 1.6. Survey results: Approach to VAs and VASPs by FATF/FSRB

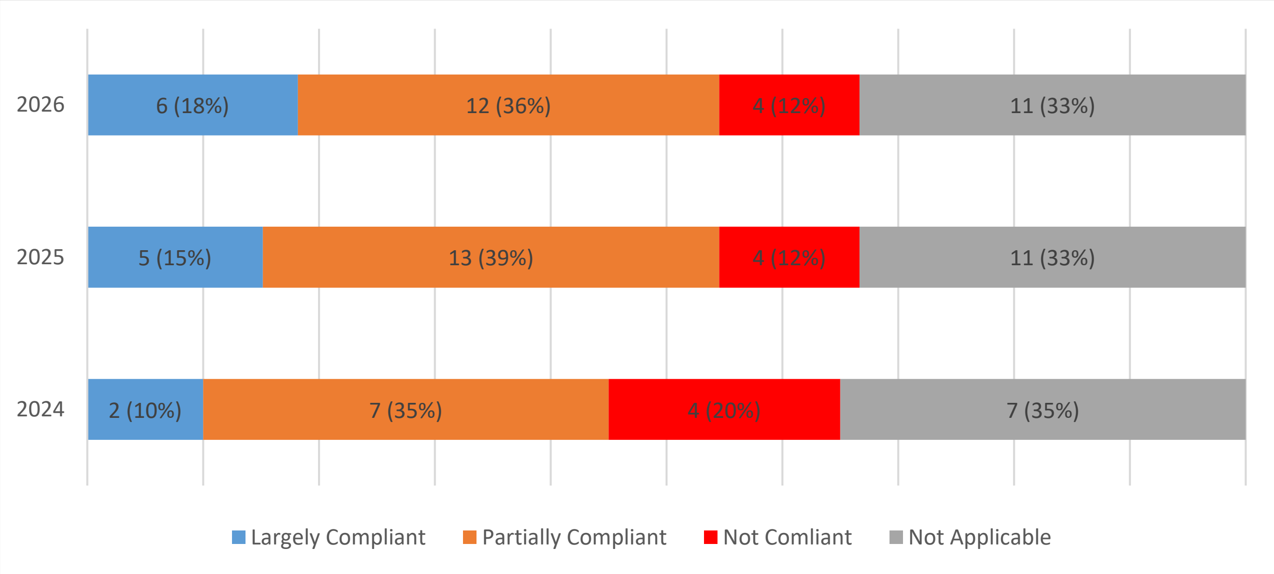


14. More than one-third of jurisdictions taking a prohibition approach reported partially prohibiting specific VA/VASP activities (36%; 12 of 33 jurisdictions), rather than fully prohibiting all VA/VASP activities (64%; 21 of 33 jurisdictions) (see Figure 1.5). While this share remains higher than in the 2024 report (30%; 6 of 20 jurisdictions), it is lower than the level reported in 2025 (48%; 16 of 33 jurisdictions), suggesting no clear upward trend toward partial prohibition.
15. Across jurisdictions, partial prohibition approaches are reflected in regulatory approaches that do not fully prohibit virtual assets and VASPs, but instead impose targeted restrictions. In particular, the use of virtual assets as a means of payment is frequently prohibited, while limited use for investment or trading is allowed under controlled frameworks. Many jurisdictions are incorporating VASPs into AML/CFT regimes, subjecting them to licensing, registration, and supervisory requirements, while imposing additional restrictions on higher-risk activities such as anonymity-enhancing services, privacy coins, mining, or custody. At the same time, some jurisdictions maintain outright bans or de facto prohibitions, whereas others are progressively developing regulatory frameworks through new legislation, sandbox initiatives, or alignment with models such as MiCA. Overall, there is a converging regulatory pattern toward restricting payment functions while integrating virtual asset activities into formal regulatory and supervisory systems.
16. Assessment results indicate that successfully prohibiting the use of VAs and VASPs is still challenging (see Figure 1.7). Six jurisdictions partially or fully prohibiting the use of VAs and VASPs have been assessed as largely compliant with the FATF standards. Although an increasing number of jurisdictions adopting a prohibition approach have conducted risk assessments, many continue

to face challenges in conducting a comprehensive and effective risk assessments. Recent results indicate that only one jurisdiction taking a prohibition approach has fully met the relevant R.15 requirement (R.15 sub-criteria 15.3).

17. Jurisdictions taking a prohibition approach have reported increased supervisory or enforcement activity against VASPs operating illegally within their jurisdiction. 16 of 21 jurisdictions explicitly prohibiting the use of VAs and VASPs reported taking such actions, compared with 9 of 17 in the 2025 Targeted Update and 9 of 14 in the 2024 Targeted Update. However, implementation remains uneven.

Figure 1.7. Assessment results: Compliance with R.15 – 33 jurisdictions taking a prohibition approach to VAs and VASPs

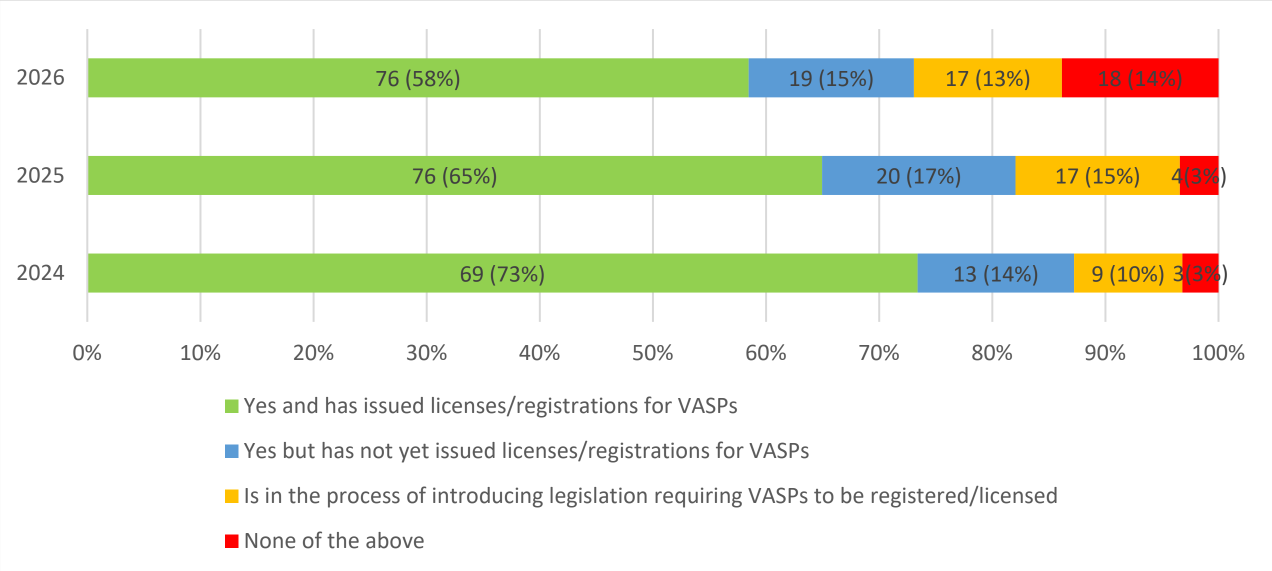


2.4.2. Licensing/Registering VASPs and taking enforcement and supervision actions

18. Jurisdictions have developed licensing or registration frameworks for VASPs, although progress in operational implementation remains uneven. 73% of respondents (95 of 130), excluding those that prohibit or plan to prohibit VASPs entirely, report that they require VASPs to be licensed or registered. However, progress in actual licensing or registration appears more limited. In the 2026 survey, 58% of respondents (76 of 130) reported having licensed or registered a VASP in practice, compared with 65% (76 of 117) in 2025. While many respondents have implemented VASP licensing or registration requirements as part of their AML/CFT frameworks, several jurisdictions do not yet have operational licensing or registration frameworks. This gap is also reflected in assessment results, as only 40% of assessed jurisdictions (59 of 149) satisfactorily require VASPs to be licensed or registered (i.e., criterion 15.4 is rated met or mostly met; see Figure 1.3). This is similar to the findings of the 2025 Targeted Update, which also noted that assessment results may not fully reflect updates captured in survey responses. The difference may also reflect methodological differences or reporting inconsistencies in self-reported survey data.

19. Still, jurisdictions report advancements in conducting supervisory inspections and taking enforcement actions or other supervisory actions against VASPs compared to 2025. This data may require further analysis to fully understand trends given the mismatch between data from survey responses and from FATF assessments, as noted above, and given some confusing survey responses. For example, some countries reported conducting an inspection but also noted that they had not licensed or registered a VASP in practice. Still, trends are outlined below to indicate changes year over year. A majority of the 95 jurisdictions that reported requiring VASP licensing or registration also reported conducting supervisory inspections of VASPs (81%; 77 of 95) and taking enforcement actions or other administrative actions against VASPs (71%; 67 of 95). This indicates a higher reported proportion of supervisory inspections than in 2025, when 73% of jurisdictions reported having conducted such inspections (70 of 96). However, reported enforcement or other administrative actions against VASPs remained slightly lower, compared with 2025 (73%; 70 of 96).
20. Of jurisdictions that assessed VAs and VASPs as high risk and do not prohibit or plan to prohibit VASPs explicitly, 10% (5 of 50 respondents) do not yet have legislation in force requiring VASPs to be registered/licensed, similar to the findings in the 2025 and 2024 Targeted Update reports.

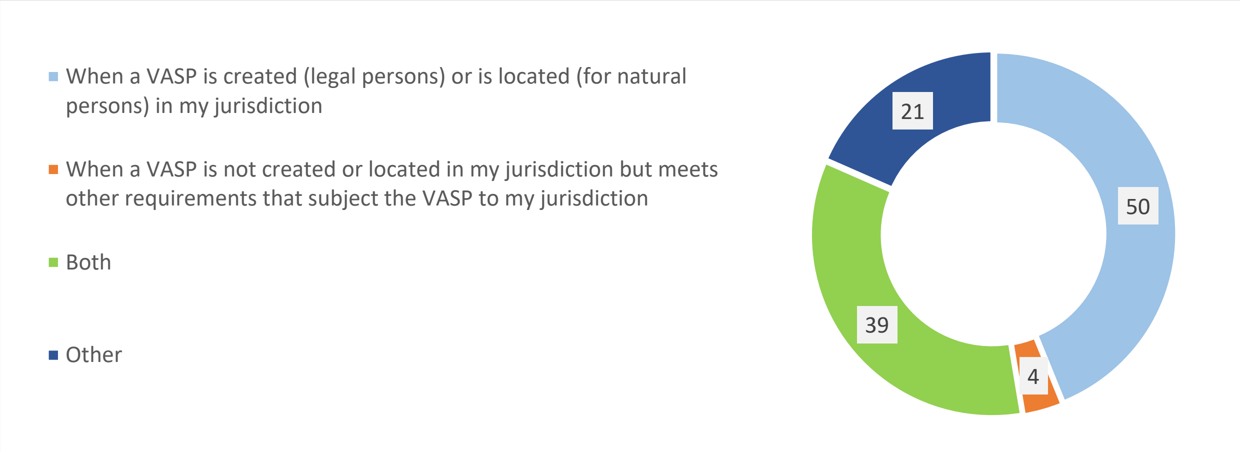
Figure 1.8. Survey results: Does your jurisdiction have legislation in force requiring VASPs to be registered/licensed?



21. The FATF Standards state that jurisdictions should require VASPs to be licensed or registered if they are physically located or incorporated in their jurisdiction. Around two-fifths of jurisdictions with VASPs licensing or registration requirements (44%; 50 of 114) report meeting this standard, requiring VASPs to be licensed/registered if VASPs are created (legal persons) or located (natural persons) in their jurisdictions (see Figure 1.9). Approximately a third of jurisdictions (34%; 39 of 114) reported taking a more extensive approach by requiring offshore VASPs (that are not created or located in their jurisdictions) to be licensed/registered if VASPs meet certain other requirements. For further analysis and insights on this issue, jurisdictions may refer to the targeted report, Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers.[10]

[10] Understanding-Mitigating-Risks-Offshore-VASPs.pdf.coredownload.inline.pdf

Figure 1.9. Survey results: Does your jurisdictions require VASPs to be registered/licensed:



22. Despite the progress noted above, jurisdictions continue to struggle with the licensing or registration process, in particular identifying natural persons or legal entities that conduct VASP activities. This highlights the continued need for information, expertise-sharing and technical assistance, particularly from FATF members (as representatives of the global standards setter).

2.5. Implementation of the FATF's Travel Rule

23. The Travel Rule applies the FATF's payment transparency requirements (FATF Recommendation 16) to the VA context. The Travel Rule requires VASPs and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when engaging in payments or value transfers, including VAs and hybrid payment chains.

24. Jurisdictions have made progress on implementing the Travel Rule. For the 2026 survey, 83% of respondents (91 of 109 jurisdictions) have passed legislation implementing the Travel Rule (see Figure 1.10), up from 73% (85 of 117) in 2025. An additional 11 of 109 jurisdictions reported being in the process of implementing the Travel Rule, compared to 14 of 117 jurisdictions in 2025.

Figure 1.10. Jurisdictional Implementation of the Travel Rule

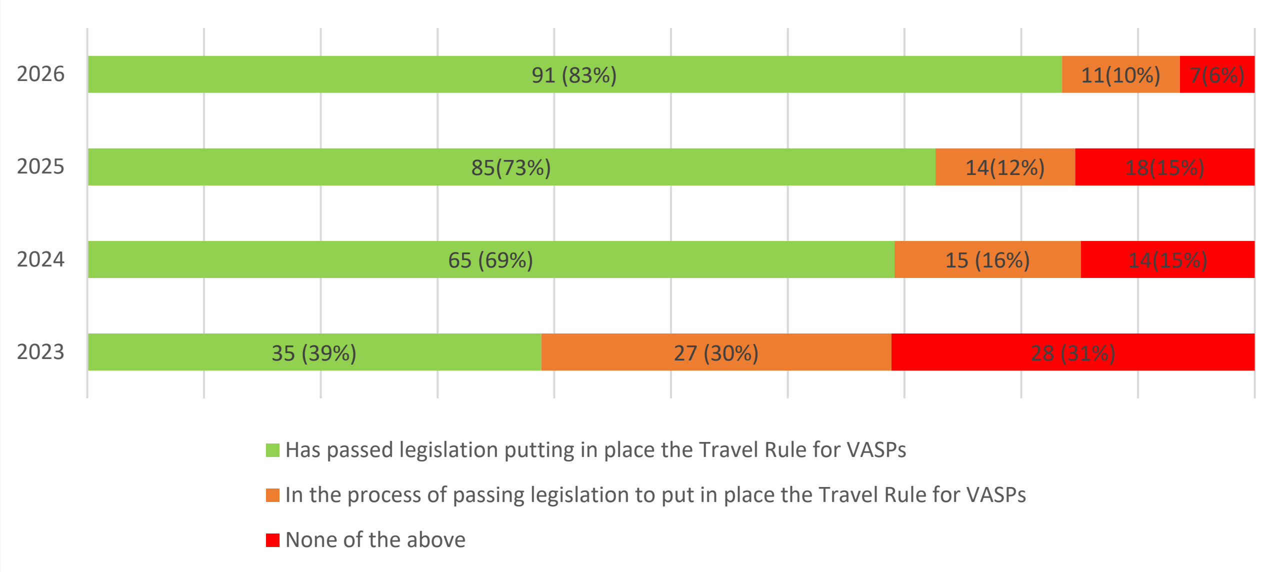
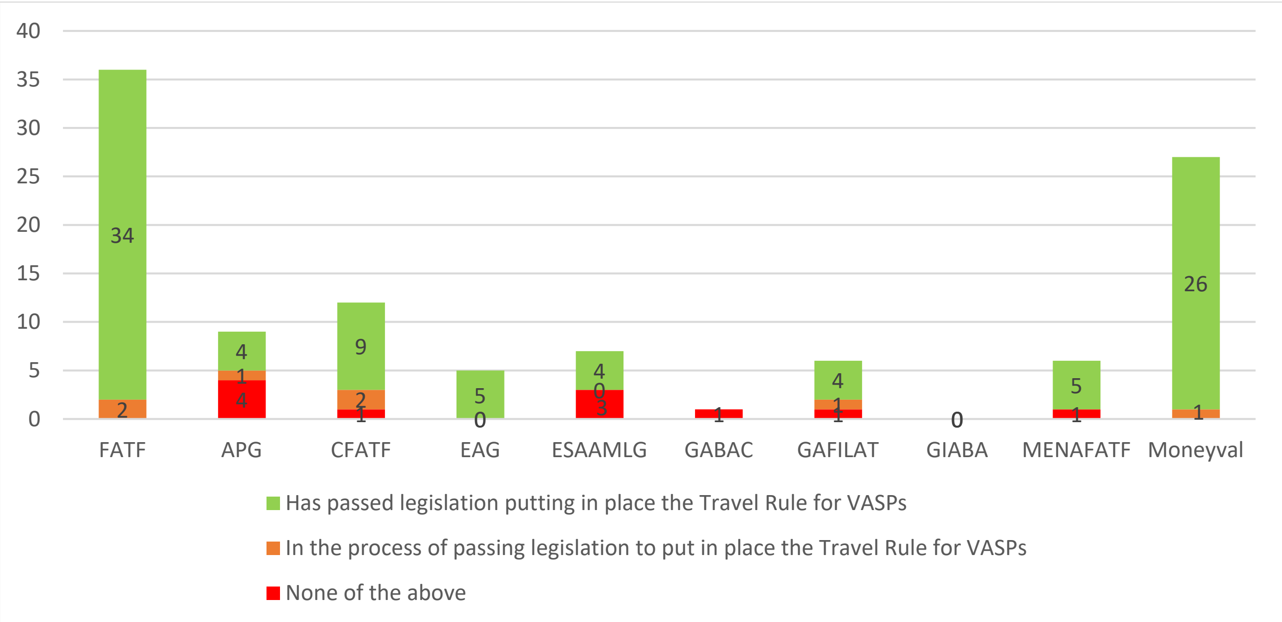


Figure 1.11. Jurisdictional Implementation of the Travel Rule by FATF/FSRB Region



25. Experience in supervising and enforcing the Travel Rule remains limited, although current results show progress compared to the 2025 results. Slightly more than half of the 91 jurisdictions (60%; 55 of 91) that have passed legislation implementing the Travel Rule have not yet issued findings or directives or taken enforcement or other supervisory actions against VASPs focused on Travel Rule compliance. This likely reflects that many jurisdictions have only recently enacted Travel Rule legislation and are currently focused on establishing supervision frameworks in this new area.

Jurisdictions may also be focusing on engaging with VASPs, have ongoing enforcement cases, or working with VASPs to remediate shortcomings. Still, the low number of enforcement actions may also be a reflection of the challenges detailed in the FATF's Best Practices in Travel Rule Supervision report.[11]

26. The persistent gaps in Travel Rule implementation remain a serious concern. As the effectiveness of the Travel Rule depends on consistent, effective and global implementation and enforcement, jurisdictions that have introduced the Travel Rule should rapidly operationalise it, including through effective supervision and enforcement in case of non-compliance. To address this, the FATF has published the Best Practice in Travel Rule Supervision paper which provides further guidance.

2.6. FATF work to accelerate global implementation of R.15

27. In addition to the VACG Roadmap activities to monitor progress on the implementation of R.15 and updating the table of jurisdictions with materially important VASP activity, the FATF Secretariat has participated in several FSRB plenaries and conducted other outreach with international partners. As mentioned in section one, a VACG symposium was held in December 2025, to support implementation of Recommendation 15 by jurisdictions, including those with materially important VASP activity. More than 400 participants from over 80 jurisdictions and FATF observer organisations attended the 2025 December VACG symposium. The key objective of this initiative was to highlight the risks associated with offshore VASPs, examine challenges in their regulation and supervision, identify emerging good practices to prevent their misuse, and gather feedback on FATF's ongoing work, including potential operational and policy responses.
28. This built upon a virtual meeting held in September 2025, where the VACG convened VACG members, Global Network members, and relevant international organisations, to discuss stablecoins and offshore VASPs, focusing on risks, vulnerabilities, regulatory and enforcement challenges, and emerging good practices. Key issues included the growing ML/TF/PF risks of stablecoins, particularly through unhosted wallets, and the challenges in supervising and obtaining information on offshore VASPs exploiting regulatory arbitrage. The FATF remains committed to working with jurisdictions to facilitate the implementation of R.15 and mitigate abuse of VAs and VASPs by illicit actors.

[11] Best-Practices-Travel-Rule-Supervision.pdf

SECTION TWO: ML/TF/PF Risks

2.1. Use of VAs for predicate offences, money laundering, terrorist financing and proliferation financing

2.1.1 Organised Crime Groups' VA-Enabled Fraud

29. Organised crime groups (OCGs), such as Cambodia-based scam centres, have emerged as significant generators of illicit proceeds involving virtual assets (VAs). These operations, commonly associated with investment fraud schemes often referred to as "pig butchering," target victims globally through sustained social engineering, inducing them to transfer funds to fraudulent investment platforms, which are subsequently diverted to wallets controlled by criminal networks. Analysis from competent authorities and international organisations indicates that such activities have generated multi-billion USD proceeds annually, with funds rapidly laundered through complex VA transaction chains involving multiple unhosted wallets, over-the-counter (OTC) brokers, and regionally based financial service providers.[12] Entities linked to these operations have been subject to sanctions and law enforcement actions across multiple jurisdictions. Notably, competent authorities found that a Cambodia-based financial services conglomerate laundered at least USD 4 billion in illicit proceeds between August 2021 and January 2025, functioning as a critical node connecting cyber-enabled fraud networks, underground banking infrastructure, and VA-based money laundering pipelines.[13]
30. Beyond serving OGC-driven fraud networks, a Cambodia-based financial services conglomerate was extensively exploited by DPRK-affiliated actors, a major PF threat, to launder virtual asset stolen through state-sponsored cyberattacks. Of the USD 4 billion in aggregate illicit proceeds processed, at least USD 37 million has been attributed to DPRK cyber heists with proceeds assessed as directly supporting the DPRK's WMD and ballistic missile programmes in violation of applicable UN Security Council Resolutions.[14] This intersection of OGC-driven fraud and proliferation financing (PF) within a single financial intermediary illustrates the convergence risk inherent to jurisdictions with deficient AML/CFT frameworks, and demonstrates the extent to which regionally embedded entities with inadequate KYC and AML controls can simultaneously serve multiple categories of illicit actor.
31. Spain's Operation Borrelli further illustrates the use of VAs in large-scale investment fraud and laundering outside the Cambodia-based scam centre context. In June 2025, the Spanish Guardia Civil, supported by Europol and authorities from Estonia, France and the United States, dismantled a cryptocurrency investment fraud network that allegedly laundered approximately EUR 460 million from more than 5 000 victims worldwide.[15] The network used a Hong Kong-based corporate and banking structure to present itself as a legitimate foreign exchange and virtual asset investment business, while collecting funds through cash, bank transfers and virtual asset transfers and moving the proceeds through payment gateways and exchange accounts held under different names. The case demonstrates how VAs may serve both as the fraud lure and as a laundering channel, while also highlighting the increasingly transnational and segmented structure of organised fraud networks.

---

[12] Cyberfraud in the Mekong reaches inflection point, UNODC reveals

[13] U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia | U.S. Department of the Treasury

[14] Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin

[15] Crypto investment fraud ring dismantled in Spain after defrauding 5 000 victims worldwide - Fraudsters laundered EUR 460 million in illicit proceeds | Europol

32. Taken together, these cases reflect the increasing industrialisation of VA-enabled fraud and its structural convergence with human trafficking, PF, sanctions evasion, and cross-border money laundering, both within dedicated scam compounds and through broader transnational investment fraud networks. They underscore significant and ongoing challenges for competent authorities, financial institutions, and VASPs in detecting and disrupting laundering flows associated with such schemes, while also highlighting systemic risks arising from uneven implementation of the FATF Standards, particularly with respect to VA service providers operating in or through jurisdictions with weak supervisory frameworks. Stronger multilateral enforcement, enhanced information-sharing mechanisms, and accelerated implementation of FATF Recommendation 15 across all relevant jurisdictions remain critical to disrupting this typology at scale.

2.1.2. Cross-Cutting Risks in VA-Enabled Illicit Finance

33. Dialogue with private sector reveals that proliferation financing, terrorist financing and sanctions evasion risks involving digital assets are increasingly converging around shared infrastructure and repeatable operating models. Sanctions evasion networks are moving from domestic exchanges toward distributed offshore intermediaries, global exchanges, OTC brokers and stablecoin payment rails, which can also be used to finance proxy groups and procure weapons, drone components and dual-use goods. The DPRK continues to exploit vulnerabilities not only in VASPs and DeFi protocols, but also in the wider third-party infrastructure on which these services rely, including RPC nodes and multi-signature security providers, while laundering proceeds through bridges, unhosted wallets and OTC networks. In relation to terrorist financing, the use of Tron-based USDT, as well as the emergence of services that obscure gas-fee funding patterns and make investigations more difficult, alongside crypto donation campaigns linked to lone actors and small cells that may provide early indicators of planned attacks. These trends suggest that PF, TF and sanctions evasion should not be viewed as isolated risks, but as interconnected activities enabled by common digital asset rails and supporting infrastructure. This underlines the importance of sustained education, stronger law enforcement capabilities, public-private information sharing, real-time disruption mechanisms, and a more outcome-focused approach to targeted financial sanctions in the digital asset ecosystem, including engagement with centralised and decentralised services, third-party technology providers, social media platforms and traditional financial institutions.
34. These convergence risks may be amplified by the increasing abuse of AI, which is emerging as a risk factor across the lifecycle of fraud, hacking and money laundering. Recent investigative cases indicate that attackers have used synthetic profiles and deepfake video interviews in AI-enabled recruitment scams to build victims' trust, before inducing them to install malware or grant wallet access, resulting in the theft of more than USD 1 million in virtual assets, primarily stablecoins. AI coding assistants and AI agents may also be used to analyse smart contract vulnerabilities, generate exploit code and identify attack paths at the internal transaction level, thereby increasing the speed and precision of attacks against DeFi protocols and cross-chain infrastructure. Once stolen, such assets can be rapidly moved and fragmented through stablecoins, DEXs, bridges and multiple VASPs, making tracing and freezing more difficult. The use of open-weight AI models and self-hosted GPU infrastructure may further enable criminals to bypass the safeguards of commercial AI platforms and automate social engineering, exploit development and fund-flow design. Authorities should see AI-enabled virtual asset crime not merely as a technical threat, but as a structural factor that can amplify ML/TF and sanctions-evasion risks, and should strengthen risk-based supervision of the VASP, DeFi and stablecoin ecosystem, taking into account controls against deepfakes and synthetic identities, AI-native investigative capabilities, and public-private information-sharing mechanisms.

2.2. Stablecoins

35. A particularly notable development in the misuse of virtual assets within VA-enabled fraud ecosystems is the deliberate issuance of proprietary stablecoins specifically designed to circumvent law enforcement intervention. In one significant case, a Cambodia-based financial services conglomerate, identified as a key money laundering node for transnational organised crime networks, launched a USD-pegged stablecoin marketed as immune to asset freezing and outside the oversight of traditional regulatory authorities. This contrasts with standard practices among some legitimate stablecoin issuers, which typically retain the technical ability to block transactions or to freeze and seize/burn tokens in wallets at the request of competent authorities. This capability gap was exploited following an instance in which a third-party stablecoin issuer froze assets valued at over USD 29 million held in a wallet linked to the same conglomerate due to suspected illicit activity, demonstrating the direct causal link between regulatory exposure and the deliberate development of freeze-resistant VA infrastructure.[16] The stablecoin was issued across multiple public blockchains as well as a proprietary chain, further complicating asset tracing and cross-chain monitoring by competent authorities. This typology illustrates an emerging and significant risk whereby obligated entities, including VASPs, may be unable to rely on issuer-level asset freeze/burn mechanisms as a compliance safeguard, and underscores the need for jurisdictions to ensure that stablecoin issuance arrangements are subject to robust AML/CFT requirements, including the technical capacity to comply with lawful blocking, freeze and seizure orders.[17]
36. This pattern of deliberate regulatory arbitrage is not confined to fraud-related networks. As documented in the FATF's targeted report on stablecoins and unhosted Wallets[18], terrorist organisations, including ISIL and Al-Qaeda, increasingly favour stablecoins over Bitcoin, exploiting rotating wallet addresses, micro-splitting of funds, and multi-hop transfers through VASPs and OTC brokers with minimal CDD requirements, while further pairing stablecoins with decentralised finance tools and unhosted wallets to circumvent compliance controls.

2.3. P2P Transactions via Unhosted Wallets

37. P2P transfers via unhosted wallets present elevated illicit finance risks, as such transactions occur directly between parties without involvement of a regulated intermediary, thereby falling outside AML/CFT/CPF obligations. While transactions on public blockchains remain technically visible, their pseudonymous nature enables threat actors to obscure attribution through layered unhosted wallets transactionally distant from Travel Rule-covered wallets, with risks further compounded on a cross-border basis given the near-instant settlement of stablecoins across jurisdictions. The absence of an obliged entity responsible for STR reporting in respect of such transactions represents a structural gap in the AML/CFT/CPF framework, though stablecoin issuers may play a complementary role by responding to law enforcement requests to freeze suspected wallets and, where appropriate, submitting STRs to the FIU.
38. Based on the survey results, 88% of jurisdictions (58 of 66) rated P2P transactions as high risk, while 8% (5 of 66) rated them as medium and 5% (3 of 66) as low. FATF has previously conducted market metric analysis of P2P transactions but was unable to present definitive figures due to significant

[16] https://www.federalregister.gov/documents/2025/10/16/2025-19571/imposition-of-special-measure-regarding-huione-group-as-a-foreign-financial-institution-of-primary

[17] targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

[18] targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

discrepancies in data across companies. As the 2026 survey results indicate that only 23% (31 of 133) of respondent jurisdictions indicated that they collect and assess P2P market metrics to evaluate the ML/TF/PF risks posed by unhosted wallets, it is important for jurisdictions and relevant stakeholders to continue closely monitoring the availability and accuracy of data on the scale and proportion of P2P transactions.

2.4. Offshore VASPs[19]

39. Offshore VASPs (oVASPs) are VASPs that provide services to clients in jurisdictions outside its jurisdiction of incorporation or physical location. oVASPs can be incorporated in any jurisdiction and may decide to operate across multiple markets. Where oVASPs are incorporated or physically located in jurisdictions with weak or underdeveloped AML/CFT/CPF regulatory and supervisory frameworks, for VAs and VASPs, it can increase the risk of ML/TF/PF abuse not only in the home jurisdiction but also the host jurisdictions in which the oVASP offers products and services. This risk can be compounded if the latter jurisdictions do not require licensing or registration of oVASPs because they often lack a physical or legal presence in the jurisdictions where their customers reside and may provide VA related services.
40. Some oVASPs actively solicit customers in jurisdictions where they are unlicensed or where VA activity is restricted, including by advising users to circumvent regulatory requirements through the use of VPNs or the provision of false information. Affiliate schemes, sponsoring of local events, and promotion via social media and encrypted messaging applications are commonly used to reach customers, reinforcing the appeal of offshore platforms among users with limited awareness of licensing and regulatory status. Others may actively lower KYC requirements and offer advantageous pricing by leveraging lower compliance costs, undermining a level playing field for regulated VASPs.
41. A further vulnerability arises from nested and intermediated arrangements, through which oVASPs access trading, liquidity, and fiat on- and off-ramps via accounts held at licensed onshore VASPs or FIs. While nested activity can be legitimate, oVASPs have been observed deliberately misrepresenting themselves as retail users when opening such accounts, and processing illicit transactions significantly exceeding typical retail volumes while accounting for only a marginal share of total host VASP activity. Where host VASPs maintain weak AML/CFT/CPF controls, the risks associated with nested oVASP activity are materially amplified, including exposure to sanctioned actors and enforcement action.
42. Regulatory arbitrage constitutes an additional structural risk, as oVASPs may incorporate or route customer activity through jurisdictions with weak supervisory frameworks to minimise compliance obligations, including customer due diligence and Travel Rule requirements. Such practices distort competition and undermine the integrity of domestic regulatory frameworks by converting lower compliance costs into pricing advantages.
43. Building on this risk understanding, jurisdictions have developed a range of measures to detect, regulate, and enforce obligations against oVASPs. Detection efforts draw on a combination of blockchain analytics, open-source intelligence, suspicious transaction reports from onshore VASPs and FIs. To enhance regulatory clarity, a growing group of jurisdictions have also adopted an activity-based approach to licensing, requiring oVASPs to register where they actively provide services regardless of physical presence, with regulatory anchors including targeted marketing, onboarding of residents, and use of domestic payment rails. To ensure licensing requirements include meaningful substance in-country, some jurisdictions also require oVASPs to maintain a

[19] Understanding-Mitigating-Risks-Offshore-VASPs.pdf.coredownload.inline.pdf

material local presence, including a compliance officer with unrestricted access to customer data and sufficient seniority to act independently.

44. Where oVASPs remain unresponsive or dispute territorial scope, jurisdictions have applied graduated enforcement measures ranging from public warnings and app-store takedowns to restrictions on access to domestic financial intermediaries and criminal prosecution. Effective responses have also relied on domestic coordination across supervisory, FIU, law enforcement, and tax authorities, as well as international cooperation through supervisor-to-supervisor channels and, where those are unavailable, diagonal cooperation via FIU networks such as the Egmont Group.

2.5. Decentralised Finance (DeFi)

45. As highlighted in previous Targeted Update reports, jurisdictions across the FATF Global Network continue to face significant challenges in identifying individuals or entities that exercise control or sufficient influence over DeFi arrangements. As a result, most jurisdictions have not, in practice, imposed licensing or registration requirements on DeFi arrangements that fall within the scope of the FATF Standards. Shortcomings also persist in the assessment of ML/TF/PF risks associated with the DeFi ecosystem, which may represent an increasingly significant gap as regulated entities, including financial institutions and VASPs, expand their engagement with DeFi platforms.

46. The 2026 survey results indicate that among responding jurisdictions:

   a. Only a minority (18%; 26 of 142) have assessed the risks associated with DeFi arrangements, and few jurisdictions (9%; 12 of 142) are in the process of conducting a risk assessment that includes DeFi-related risks.

   b. A large majority (93%; 132 of 142) have not identified DeFi arrangements operating in their territory that qualify as VASPs under the FATF Standards.

   c. While some jurisdictions (31%; 44 of 142) reported that their risk mitigation measures apply to DeFi arrangements, only four jurisdictions have imposed licensing or registration requirements, and just two have actually licensed or registered such arrangements in practice.

   d. Some jurisdictions (35%; 50 of 142) reported that their competent authorities have engaged with the private sector to better understand DeFi business models and associated risks.

47. Jurisdictions report persistent difficulties in identifying qualifying DeFi arrangements within their regulatory perimeter, due to their cross-border nature, frequent lack of formal legal structures, and the absence of clear regulatory anchors. Moreover, supervisory authorities face resource and capacity constraints in developing the technical expertise required to understand and analyse the complexity of DeFi arrangements, including determining where control or sufficient influence is exercised. This results in low levels of enforcement actions taken against DeFi arrangements that fall within the scope of the FATF Standards, with only one jurisdiction reporting to have taken enforcement actions in practice.

48. To address these challenges and support jurisdictions in implementing the FATF Standards effectively, the FATF has produced a Targeted Report on Regulatory Challenges from Decentralised Finance (DeFi). The report provides a detailed analysis of the characteristics, vulnerabilities, and

ML/TF/PF risks associated with DeFi arrangements and offers further guidance on how competent authorities can identify control or sufficient influence within such arrangements and apply licensing and registration requirements when appropriate.

SECTION THREE: Next Steps for the FATF and VACG

49. The FATF's work on VAs and VASPs during the previous biennium highlighted the inconsistent implementation of R.15. Many jurisdictions continue to face challenges in effectively regulating and supervising this fast-developing sector, including enforcing prohibitions. Persistent gaps include insufficient risk assessments, inconsistent application of the travel rule, and limited domestic and international cooperation to enable effective supervision, investigations and confiscation of VAs. This is particularly concerning as VAs are increasingly being used for payments as well as for investment purposes, and typologies show the misuse of the VA ecosystem for criminal purposes including sanction evasion, fraud and TF/PF.
50. The FATF will continue to monitor the implementation of R.15 and emerging risks within the virtual assets ecosystem, with particular attention to jurisdictions with significant VASP sectors, and will use its existing toolkit, including assessment, risk analysis and capacity building, to enhance the global status of compliance.

Annex A. Updated Table: Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions with materially important VASP Activity

1. Virtual assets (VAs) are inherently international and borderless, meaning a failure to regulate VASPs in one jurisdiction can have serious global implications. Organised crime groups, notably Cambodia-based scam compounds, have generated multi-billion USD in annual illicit proceeds through "pig butchering" investment fraud, depriving victims worldwide of their savings. A single Cambodia-based financial services conglomerate is reported to have laundered at least USD 4 billion between 2021 and 2025, serving as a critical node connecting fraud networks, underground banking, and VA-based laundering pipelines. The scammers themselves are often lured or trafficked into these compounds and coerced through threats of physical violence and humiliation into defrauding others. The same infrastructure has been exploited by the Democratic People's Republic of Korea (DPRK) to launder virtual assets stolen through state-sponsored cyberattacks, with proceeds directly supporting its weapons of mass destruction and ballistic missile programmes. Terrorist groups, including ISIL, Al-Qaeda and their affiliates, as well as ethnically or racially motivated terrorist entities, are also increasingly using VAs to raise and move funds globally.
2. The FATF published the first table in March 2024 – based on self-reported information – which shows the progress that FATF members and 20 jurisdictions with materially important virtual asset service provider (VASP) activities have made in implementing the FATF standards for VAs/VASPs. The 2025 update expanded the table to incorporate 9 additional non-FATF jurisdictions that newly met the materiality criteria, and the 2026 update identifies 2 further jurisdictions. These jurisdictions covered in the table account for approximately 97 percent of the global VA market. Ensuring the FATF Standards are fully implemented by jurisdictions within this group will significantly assist in reducing the risks identified above.
3. The information is based on jurisdictions' responses to the FATF's 2026 self-reported survey where relevant survey questions were posed alongside a selection of three possible answer choices (Yes/No/In Progress). From February to June 2026, all jurisdictions were asked to provide up-to-date information on their progress.
4. While the majority of jurisdictions report having made significant progress in fundamental areas of R.15, particularly conducting risk assessment and licensing/registering VASPs, gaps remain in taking supervisory and/or enforcement actions against VASPs. The recent MER/FUR assessment results also suggest that effective implementation of R.15 is still challenging.
5. The purpose of this table is to enable the FATF network to best support these jurisdictions in regulating and supervising VASPs for AML/CFT purposes and to encourage jurisdictions with materially important VASP activity to fully implement R.15 in a timely manner. The FATF and its VACG will continue to conduct outreach and provide assistance to jurisdictions, particularly those with lower capacity and materially important VASP activity to encourage and support compliance with R.15. This will be done in collaboration with FSRB Secretariats and other relevant international organisations, including those providing technical assistance and training.

6. The FATF used the same methodology adopted at the June 2023 Plenary as the basis for the Table.[20] This uses the following two criteria:

    a) Jurisdictions with materially important VASP activity, based on trading volume (over 0.25% of global trading); and/or

    b) Jurisdictions with a large virtual asset user base (top 30 jurisdictions with the highest VA ownership and VA adoption rates[21]).

7. In total, 2 non-FATF jurisdictions newly met the criteria for inclusion: 1 non-FATF jurisdictions met the first criterion (trading volume) and 1 met the second criterion (user base).
8. In line with the FATF's 2021 Updated Guidance on a Risk-Based Approach for VASPs, jurisdictions should consider the risks of virtual asset transfers with jurisdictions that have not taken steps towards regulating or banning VASPs. Subject to their own ML/TF/PF risk assessment, jurisdictions may also consider designating all VASPs from jurisdictions which do not effectively implement licensing or registration requirements as higher-risk.[22]
9. Neither the open-source data used to compile the table, nor the blockchain analytics companies' data used for verification purposes, is based on any assessment of a jurisdiction's illicit finance risks associated with virtual assets or of compliance with the FATF standards. A jurisdiction's inclusion in the table therefore carries no indication – either positive or negative – regarding that jurisdiction's degree of risk or its level of compliance with R.15.
10. The purpose of this exercise remains the same as in 2024. It aims to identify jurisdictions with materially important virtual asset sectors, so that the FATF network can best support them in regulating and supervising VASPs for AML/CFT purposes and to encourage jurisdictions with materially important VASP activity to fully implement Recommendation 15 in a timely manner.

[20] VACG ROADMAP: JURISDICTIONS WITH MATERIALLY IMPORTANT VIRTUAL ASSET ACTIVITY

[21] While the methodology as well as the criteria remain the same, the updated table uses a different inclusion threshold for userbase, as open-source information on the number of users (inclusion threshold used in the previous table) is no longer freely accessible.

[22] FATF (2021) Updated Guidance on a Risk-Based Approach for VASPs, para.199.

Table of steps taken by all FATF members and jurisdictions with materially important VASP activity towards implementing R.15

Jurisdiction	Has conducted a risk assessment covering VA and VASPs	Has explicitly prohibited the use of Vas and VASPs	Has enacted legislation/regulation requiring VASPs to be registered or licensed and apply AML/CFT measures[1]	Has required stablecoin issuers to be registered/licensed when they qualify as VASPs under the FATF Standards?	Has conducted a supervisory inspection or included VASPs in its current inspection plan	Has taken enforcement action or other supervisory action against VASPs	Has passed or enacted the travel rule for VASPs[1]	R.15 rating (where assessed against the revised FATF Standards)[3] and the date of assessment
Argentina	Yes	No	Yes	Yes	Yes	Yes	No	PC (2024)
Australia	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2024)
Austria	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2026)
Bahamas	Yes	No	Yes	Yes	Yes	Yes	Yes	C (2022)
Bahrain	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2022)
Bangladesh	Yes	Yes	N/A	N/A	N/A	N/A	N/A	PC (2020)
Belgium	Yes	No	Yes	Yes	Yes	No	Yes	NC (2025)
Brazil	Yes	No	Yes	Yes	Yes	No	Yes	PC (2023)
Cambodia	Yes	Partially prohibited	Yes	Yes	In progress	Yes	No	NC (2021)
Canada	Yes	No	Yes	No	Yes	Yes	Yes	LC (2021)
Cayman Islands	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2021)
China	Yes	Yes	N/A	N/A	N/A	N/A	N/A	LC (2020)
Colombia	Yes	Undecided	N/A	N/A	Yes	No	No	PC (2022)
Cyprus	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2023)
Czech Republic	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2022)
Denmark	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2021)
Egypt	Yes	Yes	N/A	N/A	N/A	N/A	N/A	LC (2024)

Jurisdiction	Has conducted a risk assessment covering VA and VASPs	Has explicitly prohibited the use of Vas and VASPs	Has enacted legislation/regulation requiring VASPs to be registered or licensed and apply AML/CFT measures[1]	Has required stablecoin issuers to be registered/licensed when they qualify as VASPs under the FATF Standards?	Has conducted a supervisory inspection or included VASPs in its current inspection plan	Has taken enforcement action or other supervisory action against VASPs	Has passed or enacted the travel rule for VASPs[1]	R.15 rating (where assessed against the revised FATF Standards)[3] and the date of assessment
El Salvador	Yes	No	Yes	N/A	Yes	Yes	Yes	PC (2024)
Estonia	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2025)
Ethiopia	Yes	Yes	N/A	N/A	N/A	N/A	N/A	PC (2021)
Finland	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2021)
France	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2022)
Germany	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2022)
Gibraltar	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2021)
Greece	Yes	No	Yes	Yes	Yes	Yes	Yes	N/A
Hong Kong, China	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2023)
Iceland	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2021)
India	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2024)
Indonesia	Yes	Partially prohibited	Yes	No	Yes	Yes	Yes	LC (2025)
Ireland	Yes	No	Yes	Yes	In progress	Yes	Yes	LC (2022)
Israel	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2022)
Italy	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2026)
Japan	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2024)
Kazakhstan	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2023)
Kenya	Yes	No	In progress	No	No	No	In progress	NC (2022)
Lithuania	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2020)
Luxembourg	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2023)

Jurisdiction	Has conducted a risk assessment covering VA and VASPs	Has explicitly prohibited the use of Vas and VASPs	Has enacted legislation/regulation requiring VASPs to be registered or licensed and apply AML/CFT measures[1]	Has required stablecoin issuers to be registered/licensed when they qualify as VASPs under the FATF Standards?	Has conducted a supervisory inspection or included VASPs in its current inspection plan	Has taken enforcement action or other supervisory action against VASPs	Has passed or enacted the travel rule for VASPs[1]	R.15 rating (where assessed against the revised FATF Standards)[3] and the date of assessment
Malaysia	Yes	No	Yes	No	Yes	Yes	Yes	LC (2025)
Malta	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2021)
Mexico	Yes	No	Yes	No	Yes	Yes	Yes	LC (2021)
Morocco	Yes	Yes	N/A	N/A	N/A	N/A	N/A	PC (2024)
Netherlands	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2025)
New Zealand	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2022)
Nigeria	Yes	No	Yes	N/A	Yes	Yes	Yes	PC (2024)
Norway	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2023)
Pakistan	Yes	No	Yes	Yes	No	No	Yes	PC (2020)
Panama	No	Undecided	In progress	Yes	No	No	In progress	N/A
Philippines	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2022)
Poland	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2024)
Portugal	Yes	No	Yes	Yes	Yes	Yes	Yes	N/A
Republic of Korea	Yes	No	Yes	No	Yes	Yes	Yes	N/A
Russian Federation*	Yes	Partially prohibited	Yes	No	Yes	Yes	In progress	PC (2023)
Saint Vincent and the Grenadines	No	No	Yes	No	In progress	Yes	Yes	PC (2025)
Saudi Arabia	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
Seychelles	Yes	No	Yes	No	Yes	Yes	Yes	LC (2026)
Singapore	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2026)

Jurisdiction	Has conducted a risk assessment covering VA and VASPs	Has explicitly prohibited the use of Vas and VASPs	Has enacted legislation/regulation requiring VASPs to be registered or licensed and apply AML/CFT measures[1]	Has required stablecoin issuers to be registered/licensed when they qualify as VASPs under the FATF Standards?	Has conducted a supervisory inspection or included VASPs in its current inspection plan	Has taken enforcement action or other supervisory action against VASPs	Has passed or enacted the travel rule for VASPs[1]	R.15 rating (where assessed against the revised FATF Standards)[3] and the date of assessment
South Africa	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2024)
Spain	Yes	No	Yes	Yes	Yes	Yes	Yes	N/A
Sweden	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2020)
Switzerland	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2020)
Thailand	Yes	Partially prohibited	Yes	Yes	Yes	Yes	In progress	LC (2021)
Türkiye	Yes	Partially prohibited	Yes	Yes	Yes	Yes	Yes	PC (2023)
Ukraine	Yes	No	In progress	No	No	No	Yes	PC (2020)
United Arab Emirates	Yes	No	Yes	Yes	Yes	Yes	Yes	PC (2021)
United Kingdom	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2022)
United States	Yes	No	Yes	Yes	Yes	Yes	Yes	LC (2020)
Venezuela	Yes	No	Yes	Yes	Yes	No	Yes	PC (2025)
Vietnam	Yes	Undecided	No	No	No	No	No	NC (2022)
Virgin Islands (British)	Yes	No	Yes	Yes	Yes	No	Yes	LC (2024)

Note: * The FATF suspended the membership of the Russian Federation on 24 February 2023.

[1] Jurisdictions are considered in progress of passing/enacting legislation/regulation where they have, e.g., tabled draft legislation, issued a draft law, undertaken a public consultation on draft legislation, etc.

[2] The elements in columns 3-7 (licensing/registration, inspection/supervision/enforcement, Travel Rule) are not relevant to jurisdictions that prohibit VASPs and are therefore marked as not applicable (N/A).

[3] This column refers to ratings attained by jurisdictions which have been assessed against the revised FATF Standards. It is important to note that the ratings may not reflect the current progress made by jurisdictions towards implementing the FATF Standards on VAs and VASPs, elements of which are shown in columns 3-7 based on the FATF 2026 self-reported survey (conducted from February to June 2026), For jurisdictions which have not been assessed against the revised FATF Standards on VAs and VASPs, the R.15 rating is marked as not applicable (N/A).

Source: FATF 2026 survey of the global network (conducted from February to June 2026); mutual evaluation and follow-up assessment reports; information from implicated jurisdictions.

July 2026

www.fatf-gafi.org