VA/VASP ML/TF National Risk Assessment Curaçao

2026

Table of Contents

1 Executive Summary	3
2 Scope and Methodology	3
2.1 Data Collection	4
3 Curaçao's VA and VASP Ecosystem	4
3.1 Sector Size and Client Base	4
3.2 Business Model and Risk Drivers	5
3.3 Ownership, Geography, and Customer Controls	5
4 Interaction with Other Sectors	6
4.1 Local Banks	6
4.2 International Banks	6
4.3 Money Transfer Companies	7
4.4 Online Gaming and Other DNFBPs	7
4.5 Payment Service Providers and Non-Regulated Players	7
5 Threat and Vulnerability Assessment	8
5.1 VA Wallets	8
5.2 VA Exchange Services	8
5.3 VA Payment Processing	8
5.4 Vulnerability Assessment	9
6 Mitigation Measures	9
7 Residual Risk Ratings	9
8 Action Plan	10
9 Overall Conclusion	10

1 Executive Summary

During the period October 2025 – April 2026 Curaçao conducted its first Virtual Assets/Virtual Asset Service Providers (VA/VASP) national risk assessment (NRA). The VA/VASP NRA examines money laundering (ML) and terrorist financing (TF)[1] risks associated with VA and VASPs during 2021–2025. Using the World Bank VA/VASP Risk Assessment Tool, it evaluates inherent threats, sector vulnerabilities, mitigation measures, and residual risks.

Research conducted in 2024, *The Rise of Financial Technology in Curaçao and Sint Maarten,* showed that the domestic VA/VASP market remains small. The research identified approximately nine potential VASPs in Curaçao, but only a small number of VASPs that were operational had formally registered under the AML/CFT/CFP framework. One additional operational entity had not completed registration, and another had not registered because it did not consider itself covered by the applicable VA services definition. The remaining 5 identified businesses appeared not to have started operations or had ceased operating. The CBCS actively monitors the sector's activities to ensure that no unregulated activities take place.

Traditional financial-sector exposure to VA/VASP is currently limited, none of the surveyed financial institutions, money transfer companies, designated non-financial businesses and professions or other relevant stakeholders reported offering virtual asset services or services to VASPs.

Curaçao nevertheless remains exposed to risks arising from pseudonymity, rapid technological change, rapid transfers, and the cross-border nature of virtual assets.

The business models of the VASPs revealed the following: VA exchange services, custodial VA wallet services and VA payment processing. These businesses displayed medium-high inherent money laundering and terrorist financing risks, but regulatory safeguards, supervisory oversight, customer due diligence, transaction monitoring, and reporting obligations substantially reduced inherent risk. VA payment processing through card-based channels and custodial wallet services both received medium-low residual-risk assessments.

The tool assessed the sector's overall residual ML/TF risk as medium-low, reflecting the effectiveness of existing mitigating measures.

2 Scope and Methodology

The assessment was conducted by a working group established in October 2025, with participation from public and private stakeholders. Private sector participants included local and international banks, money transfer companies (MTCs), payment service providers (PSPs), virtual asset service providers (VASPs), and designated non-financial businesses and professions (DNFBPs). Public sector participants included the Tax Authority, Financial Intelligence Unit (FIU), Curaçao Gaming Authority (CGA), Interpol,

[1] While this report mentions the risk assessment on ML and TF, reference is made to the report Terrorist financing (TF), Targeted Financial Sanctions (TFS), Proliferation Financing (PF), and Non-Profit Organization (NPO) for a more in-depth assessment of TF risks.

Public Prosecutor's Office (PPO), the Police Department. Moreover, other sectors such as the Chamber of Commerce.

The working group had two main objectives: to inform stakeholders about the NRA process and to secure their active cooperation. The Centrale Bank van Curaçao en Sint Maarten (CBCS) organized a dedicated training session in 2025 to improve stakeholders' understanding of the assessment framework, the VA market, and institutional responsibilities.

2.1 Data Collection

Data for the assessment was collected through structured questionnaires designed to obtain quantitative and qualitative information on inherent ML/TF risks, exposure levels, customer profiles, delivery channels, geographic risks, mitigating measures, and the effectiveness of AML/CFT controls. Statistical information was supplemented by narrative explanations, supervisory findings, and law-enforcement data.

- The **private-sector survey** covered local and international banks, MTCs, PSPs, VASPs, and DNFBPs, with particular attention to the online gaming sector. These sectors were surveyed to determine their use of virtual assets, relationships with VASPs, facilitation of VA transactions, and possible indirect exposure or interconnectedness within the wider financial system.
- The **public-sector survey** covered law enforcement agencies, supervisory authorities, and other competent authorities. It focused on Curaçao's institutional and regulatory framework, supervisory and enforcement capacity, policy measures, and authorities' operational experience in detecting, investigating, and mitigating VA- and VASP-related ML/TF risks.
- The questionnaire data was complemented by information from **other sources**, including publicly available internet resources and television, radio, and newspaper reporting.

Overall, the private-sector response was considered satisfactory. Responses were generally comprehensive and follow-up communication was constructive where clarification was needed.

3 Curaçao's VA and VASP Ecosystem

3.1 Sector Size and Client Base

In May 2024, the AML/CFT/CFP framework in Curaçao was amended to bring VASPs explicitly within its scope and on July 1, 2025, the National Ordinance on the Supervision of Virtual Asset Service Providers (NOSVASP) entered into force. It establishes licensing and supervisory requirements aligned with the Financial Action Task Force definition of VASPs.

Research conducted in 2024, *The Rise of Financial Technology in Curaçao and Sint Maarten,* identified nine potential VASPs in Curaçao, however after a mandatory call for registration in 2025 only a small number of VASPs that were operational had formally registered under the AML/CFT/CFP framework. One additional operational entity had not completed registration, and another had not registered because it did not consider itself covered by the applicable VA services definition. The remaining 5 identified businesses appeared not to have started operations or had ceased operating.

As a result, during the assessment period 2021–2025, the same small number of VASPs that were operational have formally registered under the AML supervisory framework. At the time of this assessment none of these VASPs have yet received a VASP license under the NOSVASP but are undergoing the licensing process and are subject to AML/CFT/CFP requirements supervision pursuant to the NORUT and NOIS. The market was characterized as small and still developing.

The VASPs started their operations from 2023 to 2025, so no client data was available for 2021 and 2022. The client base grew from some hundred customers in 2023 to approximately ten times more customers in 2025. In 2025, approximately 17 percent of clients were legal persons, and 83 percent were natural persons, indicating a predominantly retail customer base. Only 3 percent of clients were local.

The VASPs primarily provide:

- Fiat-to-VA, VA-to-fiat, and VA-to-VA exchange services.
- Custodial wallet services in which the VASP controls customers' private keys.
- Payment gateway services that allow merchants to accept virtual assets.
- Card-based solutions linked to VA balances.

The services operate mainly through hot wallets, which support real-time transactions but may create greater cybersecurity exposure than cold storage.

3.2 Business Model and Risk Drivers

The operational VASPs primarily operate centralized platforms focused on exchange, custody, and payment processing. The main inherent risk drivers are:

- Rapid and cross-border transfers.
- Online onboarding and exposure to higher-risk jurisdictions.
- Potential use of conversion services for layering or integration.
- Custody of customer assets and control over private keys.
- Cybersecurity, governance, asset-segregation, and internal-control risks.

The limited number of providers and absence of complex locally issued VA products constrain the scale of exposure. The VASPs are subject to customer due diligence, transaction monitoring, unusual transaction reporting, and record-keeping requirements, while the licensing process is expected to improve regulatory clarity and transparency.

3.3 Ownership, Geography, and Customer Controls

The ownership profile of the operational VASPs was assessed as relatively transparent. The ultimate beneficial owners include both local and non-local individuals, with the non-local beneficial owners originating from countries in the Eastern Mediterranean region; none was connected to a jurisdiction

classified as high-risk under the relevant international standards. The NRA found no structural indicators such as undisclosed controllers, trust-based concealment, or links to sanctioned entities.

Clients were distributed across 163 countries. The largest client jurisdictions were in the Eastern Mediterranean region, followed by clients in the South American region. In 2025, 8.8 percent of the client base was in sanctioned or high-risk jurisdictions. Those clients accounted for 1.6 percent of total transaction volume and 0.8 percent of total transaction value.

The VASPs reported no politically exposed persons clients during the assessment period. They also reported prohibiting transactions involving cryptocurrency mixers, tumblers, and other services intended to obscure transaction origins or beneficial ownership. Controls reportedly identify and block wallet addresses associated with known mixing services or sanctioned entities.

The VASPs use ongoing transaction monitoring, automated alerts, sanctions screening, high-risk-jurisdiction indicators, and blockchain analytics. These tools are used to trace transaction origins and destinations, identify exposure to darknet marketplaces and sanctioned wallets, and assign risk scores to wallet addresses.

Their AML/CFT/CFP frameworks include customer due diligence, enhanced due diligence, risk-based customer classification, record keeping, and internal escalation mechanisms. The VASPs have reported unusual transactions to the FIU since being subjected to the AML/CFT/CFP framework.

4 Interaction with Other Sectors

4.1 Local Banks

All six domestic banks reported that they did not provide VA services, offer custody or exchange services, or maintain direct business relationships with VASPs. This creates a clear separation between the domestic banking and VA sectors and reduces direct systemic contagion risk.

Banks cited concerns about pseudonymity, cross-border transfers, transaction speed, layering, high-risk jurisdictions, reputational exposure, regulatory uncertainty, and possible effects on correspondent-banking relationships. Their conservative approach reflects broader de-risking tendencies and a priority placed on maintaining stable international banking connections.

Indirect exposure may arise when customers fund foreign VASP accounts, receive VA-related proceeds, or conduct transactions linked to foreign VASPs. The exposure was assessed as limited and not systemically significant. Where VA-related activity is identified, banks apply enhanced due diligence, transaction monitoring, sanctions screening, escalation procedures, and risk-based customer acceptance policies.

4.2 International Banks

None of the international banks that completed the questionnaire (17) reported providing VA services, maintaining direct VASP relationships, or offering structured products linked to VAs.

Some banks reported limited, client-driven exposure involving deposits from VA investments, proceeds from foreign-platform trading, or VA activity conducted outside Curaçao. Such cases were described as isolated and immaterial relative to the sector's overall size. Additionally, banks apply in such cases enhanced due diligence, source-of-funds and, where relevant, source-of-wealth checks, enhanced monitoring, sanctions screening, and adverse-media checks.

Some international banks expressed interest in future VA-related business, subject to regulatory clarity, risk appetite, and international standards. No concrete initiatives or operational services were reported at the time of assessment.

4.3 Money Transfer Companies

Two of the three licensed money transfer companies responded to the questionnaire. Both stated that they did not provide VA services, facilitate VA exchange or custody, maintain VASP relationships, or integrate VA payment solutions into remittance platforms.

The responding companies cited higher perceived risk, regulatory uncertainty, compliance burdens, and business-model considerations. However, website information for the non-responding company indicated that it offered virtual-to-fiat off-ramping services, suggesting some integration of crypto-based transfer mechanisms.

4.4 Online Gaming and Other DNFBPs

The online gaming sector comprises approximately 533 entities. The assessment combined questionnaire responses with information from a Curaçao Gaming Authority survey, resulting in 39 responses. Direct interaction with virtual assets was generally reported as limited, but supplementary information indicated that approximately 13 percent of total revenue was generated from VA-related activities during 2021–2025.

VA-related funds are generally converted into fiat through international payment service providers and transferred to gaming operators through traditional payment channels. This reduces direct exposure but leaves source-of-funds and source-of-wealth risks, particularly where conversion occurs outside Curaçao.

Overall, the gaming sector had limited direct interaction, no direct business relationships with local VASPs, and exposure mainly through fiat funds processed by international intermediaries. Its VA-related ML/TF exposure was therefore assessed as limited.

4.5 Payment Service Providers and Non-Regulated Players

Interviewed payment service providers did not offer technologies interacting with VAs or services to VASPs. The assessment attributes this partly to the market's early stage, conservative risk appetites, reliance on cautious banking partners, and the fact that the specific PSP legislative framework had not yet entered into force.

The domestic unregulated sector was considered minimal to non-existent because VASPs are subject to licensing, AML/CFT/CFP obligations, and supervision. Some indirect exposure may nevertheless arise through foreign entities that are not subject to equivalent standards.

The CBCS identified two unregulated VASPs entities that appeared to be operating without authorization. Their activities have been assessed, and steps have been taken to ensure compliance with licensing requirements.

5 Threat and Vulnerability Assessment

5.1 VA Wallets

The wallet assessment identified medium risks arising from pseudonymity, peer-to-peer cross-border portability, and transfer speed. The absence of face-to-face contact was rated high, while traceability was rated at medium risk. Transfer of funds and circumvention of exchange controls were also high-risk areas.

Criminal accessibility was generally assessed at medium risk for mining and expenditure of funds, while collection and transfer of funds, and dark-web access have been assessed as high-risk. Bank or card funding was low risk, while cash, valuable in-kind goods were high risk, and virtual-currency funding was medium risk. Regulated and centralized environments were low risk, while decentralized environments were high risk.

Tax evasion, terrorist financing, circumvent exchange control were assessed as high risks, while disguising criminal proceeds, and difficulties in tracing and seizing assets were assessed as medium risks. The underground economy and possible integration with the financial services market also presented high economic risks, while strong provider accountability reduced risk.

5.2 VA Exchange Services

VA exchange services were assessed as generally medium-high risk. Fiat-to-VA services had a high risk for pseudonymity, while VA-to-fiat and VA-to-VA services had a medium risk for that factor. Cross-border portability and absence of face-to-face contact were generally high risk.

The transfer of funds was high risk for VA-to-fiat and VA-to-VA transactions. Circumvention of exchange controls was high risk across fiat-to-VA, VA-to-fiat, and VA-to-VA services. Regulated and centralized arrangements, traceability, and accountable providers reduced several other risks.

5.3 VA Payment Processing

Payment processing, primarily through card-based services and payment gateways, had a medium-high inherent-risk profile. Pseudonymity, cross-border portability, lack of face-to-face contact, were rated as high risk while traceability, and transfer speed were medium risk. Formal bank or card funding, regulated environments, and accountable providers were assessed as lower-risk features.

Remaining vulnerabilities included tax evasion, terrorist financing, and decentralized environments were assessed as low. Trace-and-seize, circumvention of exchange controls was assessed as medium, while other criminality-related factors were mainly medium or high risk.

5.4 Vulnerability Assessment

The overall vulnerability profile was assessed as moderate. Country risk was high, while the nature, size, and complexity of the business were low risk. Products and services, delivery methods, customer types, VA pseudonymity, rapid settlement, and dealings with unregistered overseas VASPs were medium risk. Institutions dealing with VASPs were assessed as very low-risk because of their highly conservative approach.

The assessment notes that anonymity is not permitted under the regulatory framework. VASPs were brought within AML/CFT/CFP legislation in May 2024, mandatory registration followed, and the NOSVASP entered into force on 1 July 2025. The sector remains new, with operational maturity still developing.

6 Mitigation Measures

Curaçao has a functioning AML, CFT, and CFP framework. Government-level mitigation was rated high for the comprehensiveness of the legal framework while international cooperation and financial and human resources capacity and entry controls were rated low. Supervision, customer due diligence, source-of-funds requirements, and guidance were rated medium.

VASP-level measures were rated high for shareholder-structure transparency. Governance and accountability, Compliance functions and internal controls and Staff AML/CFT knowledge were rated medium.

Measures implemented by traditional obliged entities, including financial institutions and DNFBPs, were also rated medium for risk assessment, risk mitigation, compliance functions, and internal controls.

Authorities reported established AML/CFT policies, growing awareness of VA risks, general investigative and supervisory tools, and functioning inter-agency cooperation. Specialized training, advanced blockchain analytics, dedicated guidance, and formal VA-specific coordination mechanisms remained areas for improvement. Overall mitigation effectiveness was assessed as medium to high.

7 Residual Risk Ratings

After assessing the inherent risks and the effectiveness of mitigating measures, the residual ML/TF risks associated with virtual asset activities in Curaçao were generally assessed as low to medium, with the overall residual risk generated by the World Bank VA/VASP Risk Assessment Tool assessed as medium-low.

The inherent risk for key VA activities, including custodial hot wallets, VA exchange services, and card-based VA payment processing, was assessed as medium-high. These activities are exposed to risks linked to rapid and cross-border movement of funds, pseudonymity, non-face-to-face onboarding, and the potential use of VA services to layer or integrate illicit proceeds. Particularly VA exchange services involving fiat-to-VA, VA-to-fiat, and VA-to-VA conversions present vulnerabilities because they may allow funds to move quickly between the financial system and virtual assets or across different virtual assets, potentially obscuring transaction trails.

Mitigating measures were assessed as medium to high. These include AML/CFT requirements such as customer due diligence, ongoing transaction monitoring, record-keeping, reporting of unusual transactions, and supervisory oversight. Several activity-level controls implemented by VASPs and other obliged entities were considered comparatively mature and effective, even though certain system-wide supervisory and operational capacities are still developing.

As a result, most VA activities were assessed as having a medium-low residual risk, reflecting the effectiveness of the current control framework. However, fiat-to-VA exchange services received a medium residual risk rating, mainly because of the higher exposure at onboarding and fiat on-ramp stages, where customer identity, source of funds, and links to the financial system require closer attention. This indicates that, while Curaçao's mitigating measures significantly reduce ML/TF risk, fiat-to-VA exchange remains the activity requiring the most continued supervisory focus.

8 Action Plan

As the supervisory authority of the VASP sector, the CBCS has developed an action plan aimed at further strengthening the sector's regulatory and supervisory framework and addressing the vulnerabilities identified through this assessment. This plan focuses on completing the regulatory framework, enhancing risk-based supervision, improving the quality and availability of data, expanding specialized expertise, and formalizing domestic and international cooperation. It is intended to support the effective mitigation of ML/TF risks while enabling the orderly development of a sound, transparent, and well-regulated VA sector.

9 Overall Conclusion

Curaçao's VA/VASP sector is small, newly regulated, internationally oriented, and largely separated from traditional financial institutions. Its technology, pseudonymity, rapid settlement, and cross-border reach create material inherent vulnerabilities, particularly for onboarding, exchange-control circumvention, illicit transfers, and exposure to higher-risk jurisdictions. On the other hand, the combined effect of registration and licensing requirements, AML obligations, transaction-monitoring systems, blockchain analytics, prudent banking-sector policies, and supervisory controls contributes to reducing the residual risk of most activities to a **medium-low level**.