VASP REGULATORY SANDBOX

OPERATIONAL COMPLIANCE GUIDE

TRINIDAD & TOBAGO SECURITIES EXCHANGE COMMISSION

MAY 2026

OPERATIONAL COMPLIANCE GUIDE

VASP Regulatory Sandbox

Trinidad and Tobago Securities and Exchange Commission

May 2026

Instructions for using this guide. This Guide sets out the ongoing obligations applicable to Sandbox Participants. It is grounded in the VA/VASP Act, the Sandbox Rules, the Financial Obligations Regulations, the Counter-Proliferation Financing Act and any other applicable written laws governing the Participant's operations. References in this Guide to "Sandbox conditions" mean the specific conditions attached to a Participant's Certificate of Acceptance. This Guide should be read together with those Sandbox conditions, which are binding on the Participant and shall prevail to the extent of any inconsistency between the conditions and this Guide.

Table of Contents

Glossary

Abbreviation	Full term
Act	Virtual Assets and Virtual Asset Service Providers Act, 2025 (Act No. 12 of 2025)
AML/CFT/CPF	Anti-Money Laundering / Counter-Financing of Terrorism / Counter-Proliferation Financing
CBTT	Central Bank of Trinidad and Tobago
CDD	Customer Due Diligence
CPF	Counter-Proliferation Financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIUTT	Financial Intelligence Unit of Trinidad and Tobago
FOR / FORs	Financial Obligations Regulations (as amended)
NRA	National Risk Assessment. References in this framework are to the 2025 ML/TF Risk Assessment of Virtual Assets and VASPs (VA-VASP NRA) and the 2021–2024 Proliferation Financing NRA (PF NRA).
POCA	Proceeds of Crime Act (as amended)
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TTSEC	Trinidad and Tobago Securities and Exchange Commission
VA / Vas	Virtual Asset / Virtual Assets
VASP / VASPs	Virtual Asset Service Provider / Virtual Asset Service Providers

Sandbox Authorisation

1.1. What the Certificate of Acceptance Authorises

The Certificate of Acceptance authorises Sandbox Participants ("Participants") to conduct only those virtual asset activities expressly specified therein, and only for the duration of its validity. It does not authorise the conduct of activity outside the scope of the Certificate, or any representation that admission to the Regulatory Sandbox constitutes full licensure, registration, or unrestricted regulatory approval. Sandbox admission is conditional, supervisory in nature, and subject to the limitations and restrictions imposed by the Trinidad and Tobago Securities and Exchange Commission ("TTSEC", "Commission").

Permitted activities are set out in section 4(2) of the Act and further specified in the Certificate of Acceptance, individually from the set below:

- Exchange between virtual assets and fiat currencies, section 4(2)(a)
- Exchange between virtual assets, section 4(2)(b)
- Transfer of virtual assets, section 4(2)(c)
- Participation in and provision of financial services related to an offer or sale of virtual assets, section 4(2)(e)
- Any other activity specified in the Sandbox conditions

Section 5(2) of the Act provides that the Regulatory Sandbox does not apply to the activities set out in section 4(2)(d), namely the safekeeping or administration of virtual assets or instruments enabling control over them. Participants are therefore not permitted to provide custody services within the Sandbox.

Temporary holding of customer virtual assets to complete authorised exchanges or transfer transactions may be permitted. Ongoing holding or safekeeping of customer virtual assets as a service is outside the scope of Sandbox authorisation.

1.2. What the Certificate of Acceptance Does Not Authorise

A Participant's Certificate of Acceptance does not authorise: any activity not expressly specified in it; the provision of custody as a service or the representation of Sandbox admission as full or unrestricted regulatory authorisation.

Where a Participant is uncertain whether a proposed activity, product, or service falls within the scope of its authorisation, the Participant must consult with the Commission prior to commencing such activity. The commencement of an unauthorised activity constitutes a breach of the Participant's Sandbox conditions and may also constitute a breach of the Act.

1.3. Sandbox Conditions

A Participant's Sandbox conditions, issued together with its Certificate of Acceptance, are legally binding and form part of the Participant's regulatory obligations under the Sandbox framework. The Sandbox conditions set out, amongst other things, the specific activities the Participant is authorised to conduct, the manner in which they must

be conducted, notification and reporting obligations, and any additional conditions imposed by the Commission during the duration of the Sandbox.

Each Participant must maintain a current copy of its Sandbox conditions and review those conditions prior to making any material change to business activities. A Participant must not implement any material change to its business model, products, services, or operational structure, without the prior written approval of the Commission where such approval is required under the applicable Sandbox conditions or the Act. Sandbox conditions may be amended by the Commission from time to time.

Participants must maintain an account with a financial institution licensed under the Financial Institutions Act throughout the Sandbox period, in accordance with section 9(b) of the Act.

2. AML/CFT/CPF Compliance Programme

A Participant must establish and maintain a compliance programme commensurate with the nature, scale, complexity, and risk profile of its activities. The compliance programme should be designed having regard to all applicable written laws, subsidiary legislation, sanctions measures, supervisory guidance, circulars, advisories, risk assessments, typologies, and other publications relevant to the Participant's activities.

Depending on the nature of the Participant's operations, this may include, among other things, obligations arising under the Proceeds of Crime Act, the Financial Obligations Regulations, the Anti-Terrorism Act, the Financial Intelligence Unit of Trinidad and Tobago Act, the Counter-Proliferation Financing framework, the Securities Act, applicable Economic Sanctions legislation and Orders, guidance and directives issued by the Commission, the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT"), the Central Bank of Trinidad and Tobago ("CBTT"), and other competent authorities, together with relevant international standards, recommendations, and publications.

Participants should ensure that their compliance programme remains current and is reviewed periodically to reflect legislative amendments, emerging risks, new guidance, supervisory expectations, and changes to the Participant's products, services, customers, delivery channels, technologies, and geographic exposure.

2.1. Approved Compliance Officer

A designated Compliance Officer is required to be approved by the Commission under Regulation 4(2) of the Financial Obligations Regulations.

Regulation 3(2) of the Financial Obligations Regulations recognises proportionality for smaller entities by permitting the most senior employee to act as Compliance Officer where the entity employs five persons or fewer. This provision affects organisational structure only and does not reduce the substantive AML/CFT obligations applicable to the Participant.

The Compliance Officer, whose identity must be kept in strictest of confidence by members of staff, must have: direct access to all customer due diligence and transaction records; sufficient seniority to escalate concerns to the Board or most senior decision-maker without interference; and the authority to file a suspicious transaction report, as described in section 2.5, without requiring approval from a business line.

Where the Participant may be part of an international group structure, the Compliance Officer must be responsible for Trinidad and Tobago compliance operations. They must have: direct access to all Trinidad and Tobago

customer due diligence and transaction records without depending on another group entity in another jurisdiction; sufficient seniority to compel a response from Trinidad and Tobago senior management on any compliance matter; and the authority to file a suspicious transaction report with the FIUTT without requiring approval from a group compliance function outside Trinidad and Tobago.

2.2. Operational AML/CFT/CPF Programme

A Participant must maintain a registered office in Trinidad and Tobago throughout the duration of its Sandbox participation, in accordance with section 9(c) of the Act.

Operations within the Sandbox should be guided by a documented and approved AML/CFT/CPF Compliance Programme, specific to Trinidad and Tobago operations, which at a minimum should contain:

- A risk assessment, required under Regulation 7(2) of the Financial Obligations Regulations, that identifies the specific risks the business creates, rather than a generic template
- Customer due diligence policies and procedures
- A sanctions screening procedure covering both name-based and wallet-address screening
- A transaction monitoring procedure with documented rules and thresholds
- A suspicious transaction reporting procedure with a documented decision-making process
- A Travel Rule procedure covering counterparty discovery and data transmission
- A record-keeping procedure covering retention periods and retrieval

A Participant must ensure that its risk assessment considers the money laundering, terrorist financing, sanctions, and proliferation financing risks associated with virtual asset activities, taking into account applicable laws, regulations, guidance, advisories, typologies, recommendations, and other relevant publications. This should include risks relating to sanctions evasion, proliferation financing, fraud, laundering of criminal proceeds, cross-border transfers, and other high-risk or suspicious activity involving virtual assets.

Where transaction volume, complexity, or risk makes manual review insufficient, the Participant should take reasonable and proportionate steps to utilise analytics tools capable of tracing transactions across multiple wallet hops and relevant blockchains.

The risk assessment must address counterparty VASP risk, including the basis on which other virtual asset service providers have been assessed and accepted as counterparties. The controls applied, where a counterparty VASP operates in a jurisdiction with weak or absent AML/CFT supervision or where adequate information about the counterparty's controls could not be obtained, must be documented.

> The AML/CFT/CPF Compliance Programme must reflect the threat profile identified in the 2025 ML/TF Risk Assessment of Virtual Assets and VASPs and the 2021-2024 Proliferation Financing National Risk Assessment published by the Government of the Republic of Trinidad and Tobago in 2025. A risk assessment and compliance programme that is not aligned with these documents will not meet the standard required.

2.3. Customer Due Diligence

Rule (a) of the Sandbox Rules requires compliance with the full range of AML/CFT/CPF preventive measures. These obligations must be operational upon commencement of Sandbox participation and onboarding of customers.

Participants must verify the identity of every customer, and any beneficial owner, before establishing a business relationship or conducting online transactions of value TT$6,000 or more. For virtual asset activity, identity verification must include wallet attribution. Participants must record and risk-assess the deposit and withdrawal addresses associated with each customer.

Enhanced due diligence (EDD) shall be applied where the risk assessment identifies higher risk, including in the following circumstances:

- Foreign politically exposed persons, their immediate family members, and close associates, as per FOR Regulation 20(1)
- Domestic politically exposed persons and officials of international organisations, as per FOR Regulation 20(1)
- Customers connected to higher-risk jurisdictions
- Customers whose source of funds includes virtual assets received from privacy-enhancing services or unhosted wallets
- Customers whose transaction patterns are inconsistent with their stated profile
- Any customer whose circumstances change in a manner that materially affects their risk profile

Privacy-enhancing virtual assets, including, but not limited to, Monero (XMR), ZCash (ZEC), and DASH, are treated by the Commission as inherently high-risk. Participants must apply EDD to any customer dealing in or transacting with these instruments, regardless of the apparent risk profile of the individual customer.

Participants must maintain complete CDD records for every customer, keep current and retain for a minimum of six years from the end of the customer relationship, in accordance with FOR Regulation 32(2).

In facilitating transactions, the Participant must consider the specific money laundering, terrorist financing, sanctions, and proliferation financing risks associated with that activity as part of its risk-based AML/CFT/CPF framework.

Stablecoins present heightened risk within this framework and require particular attention given the typologies identified in the FATF Targeted Report on Stablecoins and Unhosted Wallets (March 2026), including their use as settlement mechanisms in P2P transactions, layering activity, and cross-border value transfer. In assessing risks across all virtual asset activity, Participants should have regard to relevant typologies, guidance, and emerging risk indicators published by the FATF, the FIUTT, and other competent authorities.

Where a Participant identifies elevated risk associated with a virtual asset customer, wallet, or transaction pattern, the Participant must apply appropriate EDD, monitoring, escalation, and reporting measures consistent with applicable written law, the Financial Obligations Regulations, and the Participant's internal risk assessment framework.

The following are specific risk indicators warranting enhanced due diligence across all virtual asset transactions, and are of particular relevance to stablecoin transactions given the FATF's findings:

- Whether the transaction involves P2P flows that have passed through unhosted wallets before reaching the Participant

- Whether the transaction history reveals indirect exposure to illicit flows through multiple transaction hops
- Rapid cross-chain movement of virtual assets
- Frequent transfers through multiple wallets in quick succession
- Large value transfers arriving from or destined for unhosted wallets without a regulated intermediary in the chain
- Transactions linked to OTC brokers, P2P platforms, or coin-swap services in jurisdictions with weak or absent AML/CFT controls

For higher-risk customers, Participants must also periodically review and refresh CDD records to ensure information remains current and adequate, in accordance with FOR Regulation 11(1G)(b).

2.4. Ongoing Monitoring

Regulation 11(1G) of the Financial Obligations Regulations requires ongoing due diligence throughout every business relationship, encompassing both transaction monitoring and periodic review of customer due diligence records, with particular attention to higher-risk customers.

A Participant must monitor customer transactions on an ongoing basis throughout the duration of the customer relationship. Transaction monitoring must address both fiat and on-chain transactions and must be commensurate with the specific risks identified in the Participant's risk assessment, rather than relying solely on default settings or generic monitoring parameters.

Transaction monitoring rules, thresholds, and escalation criteria must be documented and supported by a clear risk-based rationale. Participants must periodically review, test, and adjust their monitoring controls to ensure that they remain appropriate to the Participant's business activities, customer base, products, services, transaction patterns, and evolving risk environment. A Participant must maintain an audit trail recording alerts that were generated, alerts that were reviewed and closed without further action, and alerts that resulted in escalation, suspicious transaction reporting, or other reporting obligations.

Where a Participant's risk assessment identifies exposure to on-chain transaction risk, including activity involving unhosted wallets, cross-chain transfers, stablecoin transactions, privacy-enhancing virtual assets, mixing or tumbling services, CoinJoin transactions, or customers in higher-risk jurisdictions, the Participant should apply blockchain analytics to deposit and withdrawal addresses associated with its customers on a risk-sensitive basis. Where the risk assessment does not identify such exposure, the Participant must nonetheless be able to demonstrate that its transaction monitoring is adequate to detect the on-chain risks its specific business creates and must reassess this position whenever its risk profile changes.

Where blockchain analytics is required, the provider must cover all blockchains and token standards relevant to the Participant's activities and must maintain, or retain access to, sanctions address lists that are updated in real time or near-real time. A Participant’s monitoring and blockchain analytics controls should be capable of identifying elevated risks associated with virtual asset activity, including:

- Obfuscation and concealment activity, including the use of mixing services, tumblers, CoinJoin arrangements, or other techniques intended to obscure the source, destination, ownership, or movement of virtual assets.
- Transaction and counterparty risk, including indirect exposure to high-risk, suspicious, sanctioned, or potentially illicit activity, rapid movement of value across multiple blockchain networks, activity involving unhosted wallets, decentralised exchange or coin-swap services, layering patterns, and transactions involving jurisdictions, counterparties, or transaction behaviour presenting elevated AML/CFT/CPF or sanctions risk.

2.5. Suspicious Activity Report /Suspicious Transaction Report (SARs/STRs)

A Participant must establish and maintain procedures for the identification, internal escalation, assessment, reporting, and recordkeeping of suspicious transactions and suspicious activity. Such procedures should be designed having regard to applicable written law and the reporting procedures, guidance, forms, checklists, and other materials issued by the FIUTT, including the reporting resources available on the FIUTT website at https://fiu.gov.tt/reporting.

A Participant must file an STR or SAR with the FIUTT within the timeframe prescribed under section 55A (3) of the Proceeds of Crime Act, that is, as soon as possible, but in any event, within five (5) days of having reasonable grounds to suspect that the funds used for a transaction were the proceeds of criminal conduct.

The assessment and determination of whether an STR or SAR should be filed must remain under the control of the Participant's Compliance Officer or other authorised internal reporting function and may not be delegated to an external service provider.

A Participant must maintain an STR/SAR register recording, at a minimum, the triggering event, alert, or circumstance giving rise to review, the date of internal escalation, the date on which the reporting determination was made, and the date of filing with the FIUTT where applicable.

> Participants must not disclose to any customer, user, counter-party or other person outside of its internal compliance team that a suspicious transaction or activity report has been or may be made, that an investigation is underway, or that property has been or may be frozen. This prohibition applies under both the Proceeds of Crime Act and the Counter-Proliferation Financing Act, 2025, and constitutes a criminal offence under each.

2.6. Sanctions Screening

A Participant must conduct screening against applicable sanctions and targeted financial sanctions measures arising under the Anti-Terrorism Act (sections 22AB and 22C), the Economic Sanctions Act, applicable Economic Sanctions Orders, the Trinidad and Tobago Consolidated List of High Court Orders maintained by the FIUTT, and any notices, directives, advisories, updates, designations, or other publications issued by the FIUTT, the Commission, or other competent authorities.

Sanctions screening must be conducted on a risk-sensitive and ongoing basis and must be capable of detecting exposure to terrorist financing, proliferation financing, and sanctions risks associated with the Participant's activities. Screening must include, where applicable, customers, beneficial owners, directors, senior officers, authorised signatories, controllers, counterparties, originators, beneficiaries, wallet addresses, transactions, and other persons, arrangements, or relationships associated with the Participant's activities pursuant to the relevant laws and regulations.

Sanctions screening must not be limited to customer onboarding alone, but Participants must also ensure that screening identifies updates to sanctions lists, changes in ownership or control, indirect exposure, wallet activity, counterparty risk, and other sanctions-related risks relevant to the Participant's business.

Participants must maintain procedures for the review, escalation, investigation, and disposition of sanctions alerts and potential matches, including procedures relating to freezing obligations, internal escalation, reporting, and engagement with competent authorities where required under applicable written law.

Where blockchain analytics or other screening tools are used, such tools should be commensurate with the Participant's activities and capable of screening relevant wallet addresses, transactions, counterparties, and other virtual asset exposure associated with the Participant's products and services.

2.7. Information Requirements for Virtual Asset Transfers

Where a Participant conducts the transfer of virtual assets on behalf of a customer, the Participant must collect, verify, record, transmit, and retain the originator and beneficiary information required under Part VA of the Financial Obligations Regulations.

Before initiating a transfer of virtual assets, a Participant acting as the originating virtual asset service provider must collect and record the following information in respect of the originator and beneficiary:

- Originator information
  - Full name of the originator;
  - Account number of the originator, where an account is used to process the transfer; and
  - One of the following identifiers:
    - residential or business address;
    - number of a Government-issued identification document;
    - customer identification number; or
    - date and place of birth.

- Beneficiary information
  - Full name of the beneficiary;
  - Account number of the beneficiary, where an account is used to process the transfer; and
  - Where no account is used to process the transfer, the unique transaction reference number or other identifier that permits traceability of the transaction.

Participants must verify originator information before executing the transfer using documents, data, or information that satisfy applicable customer due diligence requirements. Required information must accompany the transfer simultaneously with, or concurrently with, the transfer of virtual assets.

Where a Participant receives a transfer of virtual assets as a beneficiary virtual asset service provider, it must collect and record beneficiary information, verify beneficiary information in accordance with applicable customer due diligence requirements, and retain complete originator and beneficiary information associated with the transfer.

Participants must maintain procedures capable of detecting missing or incomplete information. Where required information is absent, incomplete, or cannot be obtained, Participants must apply appropriate risk-based procedures, including escalation, requests for additional information, suspension, rejection, or other measures appropriate to the circumstances.

Participants must retain complete originator and beneficiary information and associated transfer records for a minimum period of six years in accordance with Part VA of the Financial Obligations Regulations.

2.8. Record-keeping

Rule (e) of the Sandbox Rules / Section 10 of the Act requires the following records, including all versions, to be maintained on an ongoing basis:

- Incorporation documents and certificates of good standing
- Minutes of Board and committee meetings

- Financial statements for each period of Sandbox participation
- AML/CFT/CPF policies and procedures

A Participant's record-keeping systems must preserve accurate audit trails, timestamps, transaction history, and supporting documentation sufficient to reconstruct customer activity and demonstrate compliance with applicable written law. Participants must retain the following for a minimum of six years:

- All customer due diligence records, including identity verification documents and beneficial ownership information
- All transaction records, including blockchain transaction identifiers and wallet address information
- All internal investigation records, including alert logs, triage notes, and escalation decisions
- All AML/CFT/CPF audit and assurance records
- All STR and SAR records, including the date of filing and FIUTT acknowledgement
- All sanctions screening logs

Records must be stored in hard copy or on a data server physically located in Trinidad and Tobago in accordance with section 6(3)(b) of the Act. Records must be maintained in a form that is retrievable, and capable of production to competent authority on request.

All records accumulated during the Sandbox period must be retained until six years from the date of expiry, revocation, or cancellation of the Participant's Certificate of Acceptance, in accordance with section 10(2) of the Act.

2.9. Proliferation Financing and Targeted Financial Sanctions

Compliance with AML/CFT/CPF obligations includes compliance with the Counter-Proliferation Financing Act, 2025 and the Counter-Proliferation Financing Regulations, 2025. Participants should ensure that their compliance programme, risk assessment, transaction monitoring, sanctions screening, training, and record-keeping arrangements address proliferation financing risks and targeted financial sanctions obligations.

Participants should note that certain obligations under the CPF framework operate immediately and may differ from the timing applicable to standard AML/CFT reporting obligations. Upon receipt of an updated list of listed entities, Participants must determine whether any listed entity holds property with the Participant or is involved in a transaction or business relationship. Where listed property is identified, the Participant must take the actions required under applicable written law, including freezing and reporting obligations where applicable.

Participants must also ensure that procedures exist for identifying attempted transactions involving listed entities, escalating potential matches, making required notifications to the FIUTT, and preventing unauthorised disclosures relating to reports, investigations, or freezing actions.

The compliance programme and training framework should specifically address proliferation financing risks, targeted financial sanctions, and the procedures applicable under the CPF framework. Participants are directed to the Counter-Proliferation Financing Act and the Counter-Proliferation Financing Regulations for the full statement of applicable obligations.

3. Segregation of Customer Assets

Participants must ensure that customer assets are segregated from the Participant's own assets and remain clearly identifiable in the Participant's books, records, accounts, and, where applicable, wallet structures. Customer assets must not be used for the Participant's own account, pledged, lent, rehypothecated, or otherwise deployed for the benefit of the Participant.

Customer assets should be maintained separately from the Participant's operating funds and must not be commingled with business assets or used for the Participant's operational purposes.

Where customer virtual assets are temporarily held as an incident of an authorised exchange or transfer transaction, such assets must remain identifiable as customer assets throughout the transaction process and appropriate records must be maintained.

Participants must maintain reconciliation procedures and controls sufficient to identify customer asset holdings, detect discrepancies, and demonstrate compliance pursuant to Section 1.1 above.

3.1. Safeguarding and Administration Restrictions in Practice

Pursuant to Section 1.1, Participants are not authorised to provide custody of virtual assets as a service. In practice this means:

- Participants must not operate a hosted wallet service under which private keys are held on behalf of customers as a continuing arrangement
- Participants must not hold a customer's virtual assets beyond the period necessary to execute a specific exchange or transfer transaction
- A Participant must not enter into any contract under which it undertakes to safeguard customer virtual assets on an ongoing basis
- Participants must not offer staking, lending, or yield services that involve holding of customer virtual assets beyond the execution of a specific transaction

As a test, if a Participant can move customer assets without the customer's authorisation, it is offering custody as a service. If at any point during the Sandbox period, a Participant identifies that it is holding customer virtual assets in a way that amounts to ongoing safekeeping, said Participant must cease that activity and notify the Commission immediately.

4. Disclosure, Marketing and Regulatory Representations

4.1. Representation of Sandbox Status

Participants should ensure that customer-facing materials, platforms, communications, and other public-facing content accurately describe the Participant's Regulatory Sandbox status and do not misrepresent the nature or scope of the Participant's authorisation.

Any reference to Sandbox participation should be clear and prominent and should not be obscured, diluted, or embedded solely within general terms and conditions or similar legal documentation. Communications describing Sandbox participation should make clear that the Participant's authorisation is conditional, subject to applicable restrictions and limitations, and valid only for the period specified in the Participant's Certificate of Acceptance and applicable Sandbox conditions.

Participants must not represent Sandbox admission as full regulatory authorisation or otherwise misstate the scope of activities, customer classes, geographic reach, restrictions, or conditions applicable to their operations.

Where a Participant's Certificate of Acceptance, Sandbox conditions, permitted activities, or operational limitations change, customer-facing representations relating to regulatory status should be reviewed and updated as appropriate. These expectations apply throughout the Participant's period of Sandbox participation.

4.2. Marketing and Communications Standards

Rule (f) of the Sandbox Rules requires that all marketing and promotional material be fair, clear, transparent, and not misleading. This applies to all communications with customers and prospective customers, including website content, social media, email, and in-app messaging.

Participants must not:

- Represent Sandbox admission as full regulatory authorisation in any communication
- Make misleading representations about yield, returns, asset backing, or the protection afforded to customer assets
- Use the Commission's name or logo in a way that implies Commission endorsement of its products or services
- Make claims about its regulatory status in other jurisdictions that are inaccurate

Fee schedules and pricing should be disclosed to customers in advance of any transaction. All charges should be reconcilable by the customer from the disclosed schedule.

4.3. Complaints Handling

A Sandbox Participant must establish and maintain a complaints-handling mechanism that is accessible to customers without charge and that provides clearly defined timeframes for the acknowledgement, investigation, and resolution of complaints. The Participant must maintain a register recording all complaints received, the category of each complaint, the outcome of the matter, and, where identifiable, the underlying root cause.

Where a customer files a complaint in relation to the Act or the Participant's conduct under it, the Participant must notify the Commission in writing within ten days of becoming aware of the complaint, in accordance with section 10(3)(b)(vi) of the Act. Within a further seven business days of that notification, the Participant must furnish the Commission with a written report setting out the particulars of the complaint and the mitigating measures the Participant intends to undertake, or has undertaken, in accordance with section 10(4) of the Act.

For the avoidance of doubt, the notification obligation under section 10(3)(b)(vi) applies to complaints relating to the Act and the Participant's regulated activities under it. It is distinct from the general obligation to maintain a complaints register, which captures all complaints received regardless of whether they engage the Act. Both obligations apply concurrently and neither discharges the other.

5. Scope of Authorisation

5.1. Conducting Authorised Activities

A Participant must conduct only those virtual asset activities expressly authorised under its Certificate of Acceptance. The regulatory framework applies based on the substance and character of the activity being conducted. Where a Participant conducts an activity falling within section 4(2) of the Act in or from within Trinidad and Tobago, the Participant must be authorised to conduct that specific activity under its Sandbox admission. The manner in which an activity is described, labelled, or marketed does not determine whether it falls within the regulatory scope of the Act.

Participants must assess their activities on an ongoing basis to ensure that they remain within the scope of their existing authorisation. Where a Participant develops a new product or service, modifies an existing service, or implements technological or operational changes that may alter the nature or character of its activities, the Participant must determine whether such changes remain within the scope of its existing authorisation before commencing the activity.

5.2. Considering Variations

A Participant must obtain the Commission's prior written approval before commencing any activity that falls outside the scope of its existing Certificate of Acceptance. Prior approval, per 10(3) of the Act, is required where a Participant intends to:

- introduce a service or activity not currently authorised;
- materially change its business model or operational structure;
- deploy a new smart contract, protocol, or technological framework that materially alters the nature of the service being provided; or
- introduce a new product or activity that may fall within a different category of virtual asset activity under section 4(2) of the Act from those currently authorised.

The activities above serve as a non-exhaustive listing and is only provided as examples of activities where the Commission's approval would be required.

> Do not wait until an examination or supervisory review to assess whether an activity falls outside the scope of its authorisation. Where any uncertainty exists, the Participant should consult with the Commission before commencing or continuing the activity.

6. Governance and Senior Officer Obligations

6.1. Board Responsibility

Boards carry ultimate responsibility for the conduct of virtual asset activities in the Sandbox. This is not a delegable responsibility. The Board must:

- Approve and keep under review a documented risk appetite statement addressing virtual asset, ML/TF, PF, market integrity, technology, and consumer-protection risks
- Receive and consider substantive reports on virtual asset risks at least quarterly
- Approve AML/CFT/CPF programme and risk assessment
- Approve wind-down plan and review it at least annually
- Satisfy itself that the Compliance Officer has the independence, authority, and resources to perform their functions effectively

Board decisions on material compliance and risk matters must be recorded in minutes. The Commission may request Board minutes at any time.

A Participant must have in place policies and procedures, satisfactory to the Commission, to avoid, mitigate and deal with conflicts of interest between the Participant and its customers, and between customers of the Participant, in accordance with section 9(g) of the Act.

6.2. Fit and proper obligations

Senior officers must satisfy the Commission's fit and proper requirements on an ongoing basis. Any circumstance that may affect the fitness or propriety of a senior officer, including regulatory action, enforcement proceedings, criminal matters, insolvency events, or other material developments in any jurisdiction, must be reported to the Commission promptly.

A Participant must not permit a person who no longer satisfies the applicable fit and proper requirements to continue exercising senior officer functions, where doing so would be inconsistent with the Act, the Participant's Sandbox conditions, or any direction issued by the Commission.

7. Technology, Cybersecurity, and Operational Resilience

7.1. Cybersecurity

Participants are required under section 9(d) of the Act to ensure that the recording, storing, protecting and transmission of data is conducted in accordance with applicable written law, including data protection legislation. This requires:

- An information security policy covering systems, data, and third-party access
- Multi-factor authentication on all administrator and privileged accounts
- Absence of shared accounts
- A documented access control policy with quarterly review of who holds privileged access
- A cyber-incident response plan that is tested annually.
- A log of all cyber incidents during the Sandbox period, with resolution status

Dependent on the scale of operations, additional measures such as independent annual penetration testing, may be expected of participants.

Participants should refer to the CBTT's Cybersecurity Best Practices Guideline (2023), available at www.central.bank.org.tt, as a baseline reference for cybersecurity governance applicable to regulated financial institutions in Trinidad and Tobago. It also provides a Cyber Incident Reporting Form and a Self-Assessment Checklist.

Notwithstanding the above, Participants are expected to notify the Commission of material cyber incident, including scenarios where there are customer data loss, unauthorised system access, asset loss, key compromise or other similar significant events, within 1 business day, in writing or via email.

7.2. Operational Resilience

Participants are required under section 9(f) of the Act to plan for business continuity and disaster recovery in the event of an incident or disaster. Participants must ensure such a plan covers critical business services. The plan must specify recovery time and recovery point objectives for each critical service and must be tested. The plan must address the failure of critical third-party providers, including but not limited to, cloud infrastructure, blockchain analytics, and KYC providers.

7.3. Smart Contracts and Technology Changes

Any smart contract deployed into operations must have been independently audited before deployment by a reputable provider with relevant expertise. Deployment of material changes to smart contracts or protocols without prior notification to the Commission is prohibited. All material technology changes during the Sandbox period must be recorded in a change-management log.

Where AI or algorithmic systems are in operations, including in trading, compliance, or customer-facing services, the Compliance Officer must be able to understand the outputs of those systems and must retain the ability to override automated decisions.

7.4. Third-party Providers

The use of third-party providers, including KYC vendors, blockchain analytics providers, cloud providers and liquidity providers, does not transfer regulatory obligations to those providers. Participants remain responsible for the outcomes of operations regardless of outsourcing delivery of underlying service. Due diligence must be conducted on each material third-party provider before engaging them and an outsourcing register covering all material vendors must be maintained. Participants should also ensure that all security updates for these third-party providers are deployed promptly.

8. Obligations to the Commission

8.1. Cooperation

Participants are required under section 16(3) of the Act to provide the Commission with information, explanations, documents, and access to systems and premises when requested. This obligation applies at all times, not only during formal examination. The Commission may conduct supervisory engagement, request information, or visit Participants' premises at any point during the Sandbox period.

Participants must designate a named contact who is available to the Commission on a working-day basis and who can respond to Commission enquiries promptly. If the designated contact changes, the Commission must be notified of the new contact immediately.

A Participant must maintain a registered office in Trinidad and Tobago throughout the duration of its Sandbox participation, in accordance with section 9(c) of the Act.

8.2. Reporting Obligations

Participants must file the periodic reports required by their Sandbox conditions, including AML/CFT reports, on the schedule and in the form the Commission specifies in accordance with Section 5(1)(e) of the Act. Participants are expected to notify the Commission in advance where a delay in filing is anticipated.

Participants must submit monthly transaction reports to the Commission covering the volume of transactions, number of customers, and total value of assets transacted, in the form and by the deadline specified in the Participant's Sandbox conditions.

8.3. Consequences of Breach

A breach of your Sandbox conditions or of the Act may result in the Commission taking action under section 12 of the Act, including: imposing additional conditions on your Certificate of Acceptance; suspending your Certificate of Acceptance; or revoking your Certificate of Acceptance. The Commission may also refer matters to the Director of Public Prosecutions, or other competent authorities as appropriate.

Self-reporting a breach promptly, before the Commission identifies it, is a relevant consideration in the Commission's response. Concealing or delaying the reporting of a breach is an aggravating factor.

9. Contact

Questions about Sandbox obligations or the Certificate of Acceptance should be directed to the Commission's AML Unit; email: vaspSandbox@ttsec.org.tt and other pertinent information can be accessed on the Commission's website at https://www.ttsec.org.tt/industry/virtual-assets/regulations-for-va-vasp-act/.

For urgent matters, including material breaches, cyber incidents, or regulatory actions against group entities, please contact the Commission by telephone (868) 223-2991 and follow up in writing on the same day.

END

References and Source Materials

The following sources underpin the obligations set out in this guide. They are provided so that participants can identify the international and domestic frameworks from which specific standards derive. References marked with an asterisk (*) are the primary domestic legal instruments; obligations arising under those instruments are not discretionary.

1. *Virtual Assets and Virtual Asset Service Providers Act, 2025 (Act No. 12 of 2025). Port of Spain: Parliament of Trinidad and Tobago.
2. *Rules for Sandbox Participants. December 2025. Trinidad and Tobago Securities and Exchange Commission.
3. *Financial Obligations Regulations, 2010 (as amended). Trinidad and Tobago. Sets out the AML/CFT obligations applicable to financial institutions and listed businesses, including the Compliance Officer designation requirement under Regulation 3 and 4.
4. *Proceeds of Crime Act, Chap. 11:27 (Trinidad and Tobago, as amended by the Miscellaneous Provisions (FATF Compliance) Acts of 2020, 2024, and 2025). Governs STR filing obligations, tipping off prohibition, and record keeping requirements.
5. *Anti-Terrorism Act, Chap. 12:07 (Trinidad and Tobago, as amended). Governs terrorist financing obligations.
6. *The Counter Proliferation Financing Act 2025 and Counter Proliferation Financing Regulations 2025 (Legal Notice 416 of 2025)
7. *Economic Sanctions Act (Trinidad and Tobago). Governs the domestic implementation of targeted financial sanctions including UN Security Council resolutions.
8. Trinidad and Tobago Securities and Exchange Commission, AML/CFT/CPF Guidelines for the Securities Sector (2026 edition). Sets out the Commission's specific expectations for AML/CFT/CPF compliance by regulated entities including Sandbox participants.
9. Government of Trinidad and Tobago, ML/TF Risk Assessment of Virtual Assets and Virtual Asset Service Providers (March 2026). The 2025 VA, VASP NRA establishes the domestic ML/TF threat profile that must be reflected in every participant's Business Wide Risk Assessment.
10. Government of Trinidad and Tobago, Proliferation Financing National Risk Assessment 2021,2024 (March 2026). The PF NRA establishes the domestic proliferation financing threat profile, including DPRK and Iran typologies, that must be addressed in every participant's risk assessment.
11. Financial Action Task Force, Recommendation 15 and Interpretive Note (as revised 2019). Paris: FATF. The controlling international standard for the regulation and supervision of virtual asset service providers.
12. Financial Action Task Force, Recommendation 16 and Interpretive Note (Travel Rule). Paris: FATF. Sets out the Travel Rule obligations applicable to originator and beneficiary information for virtual asset transfers.
13. Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (October 2021). Paris: FATF. Provides detailed guidance on the application of FATF Standards to VASPs, including the substance-over-form approach to DeFi, the treatment of unhosted wallets, and the VASP-to-VASP relationship standard under R.13.
14. Financial Action Task Force, Targeted Report on Stablecoins and Unhosted Wallets, Peer-to-Peer Transactions (March 2026). Paris: FATF. Establishes that stablecoins account for 84% of illicit VA transaction volume globally; identifies P2P stablecoin transfers via unhosted wallets as the primary stablecoin vulnerability; documents DPRK, Iranian, drug trafficking, and fraud typologies; recommends multi-hop blockchain analytics; and provides Annex A risk indicators for transaction monitoring calibration.
15. EU Global Facility on AML/CFT, Methodology on Virtual Assets: Comprehensive AML/CFT Framework (February 2026). Funded by the European Union; implemented by Expertise France and GIZ. The comprehensive risk assessment methodology, liquidity stress scenarios, and technology governance standards drawn upon in this guide are consistent with the EU Global Facility framework, which represents current international best practice for VASP supervision.
16. Central Bank of Trinidad and Tobago, Cybersecurity Best Practices Guideline. Available at: https://www.central,bank.org.tt/central,bank,issues,cybersecurity,best,practices,guideline/. Sets out baseline cybersecurity governance expectations applicable to regulated financial entities in Trinidad and Tobago, including access controls, incident response, and technology resilience standards.