SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Scope of External Assessment Reports

June 2023

Contents

Scope of External Assessment Reports	3
Appendix 1	5
Appendix 2	13

Scope of External Assessment Reports

1. Each virtual asset ("VA") trading platform operator applicant under the existing SFO regime and/or the AMLO VASP regime is required to submit (i) an external assessor report when submitting its licence application, and (ii) another external assessor report after an approval-in-principle has been granted. This paper sets out the scope of the expected external assessment reports.

Procedures

2. When submitting its licence application, a platform operator should submit a report on an assessment of the design effectiveness of its policies and procedures conducted by external assessor(s) ("**First-phase Assessment**").

3. During the assessment process of the licence application, the SFC will invite the platform operator to conduct process walk-through and system demonstration on each of the key risk areas.

4. After the SFC grants an approval-in-principle to the application, the platform operator can then proceed to implement any outstanding systems and controls and engage external assessor(s) to assess the full implementation and effectiveness of the policies, procedures, systems and controls on key risk areas, including conducting penetration and vulnerability tests ("**Second-phase Assessment**"). Final approval will be granted subject to the result of the Second-phase Assessment and completion of other outstanding matters (as applicable) such as arranging insurance policy, opening segregated bank accounts, injecting capital, completing admission procedures for VA to be offered, etc.

5. Requirements for the selection and appointment of external assessors:

   - Separate external assessors may be engaged for the reviews of different areas as appropriate (eg, cybersecurity and custody), depending on the external assessors' expertise, experience and track records in the field.

   - The external assessor should be independent from the applicant, its group or group companies.

   - The service provider of a particular system should not act as the external assessor for the same system.

   - The external assessor should possess the necessary expertise and technical knowledge to conduct the required assessment.

   - Capability statement of external assessor(s) should be submitted to the SFC together with the external assessment report. The SFC reserves the right to oppose the appointment of any external assessor.

6. Scope of assessment

   a) <u>First-phase Assessment - external assessment on design effectiveness</u>

   First-phase Assessment should focus on the design effectiveness of the VA trading platform's proposed structure, governance, operations,

systems and controls. The external assessor should review and assess whether the platform operator's policies and procedures are clearly written and comply with the applicable legal and regulatory requirements, including but not limited to the Guidelines for VA Trading Platform Operators and the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed VA Service Providers). Please refer to Appendix 1 for the areas to be covered.

b) Second-phase Assessment - external assessment on implementation of systems and controls

Second-phase Assessment should focus on the implementation and effectiveness of the actual adoption of the planned policies, procedures, systems and controls. Final approval of the licence application will be granted subject to, among other things, the SFC being satisfied with the result of the Second-phase Assessment. Please refer to Appendix 2 for the areas to be covered.

SFC 證監會

Appendix 1

First-phase Assessment – assessment on design effectiveness

Format of assessment report

1. The assessment report should cover the following items:

- Executive summary
- Expertise, experience and track record of the external assessor(s)
- Scope/areas of the assessment
- Limitation of the assessment
- Approach to the assessment
- Description of the relevant structures/processes/policies/procedures/ systems/control of the specific areas that have been assessed and the approach and assessment procedures carried out by the external assessor(s)
- Detailed findings and recommendations in areas of non-compliance with the applicable legal and regulatory requirements, and the actions taken (or planned to be taken together with a specified timeline) by the platform operator to rectify the matters

Areas to be covered

2. While the actual scope of areas to the covered under the First-phase Assessment may vary depending on the business and operations of a platform operator, the SFC expects the First-phase Assessment to cover, at least, the following areas:

2.1 *Part A – Governance and staffing*

(i) providing an organisational chart depicting the proposed management and governance structure, business and operational units and key human resources of the platform operator and their respective reporting lines;

(ii) confirming the adequacy and appropriateness of the proposed corporate governance and staff resources, taking into account the specific nature of VA trading activities;

(iii) with respect to personnel competency, assessing and confirming that members of the senior management of the platform operator have the relevant industry experience, qualifications, technical expertise, and know-how for the key business functions for which they are responsible;

(iv) confirming that there will be a sufficient number of suitably qualified and experienced professionals for each business function,

with supervisory and reporting responsibilities assigned to appropriate staff members;

(v) identifying the key personnel and confirming that an effective plan will be in place to mitigate key-man risks; and

(vi) confirming that members of the senior management fully understand the nature of and risks associated with the VA trading business, the applicable legal and regulatory requirements, and the extent of their own authority and responsibilities.

2.2 *Part B – Token admission*

(i) confirming that a token admission and review committee composed of the required members will be set up with a transparent, fair and properly documented decision-making process and with mechanisms for regular reporting and ongoing monitoring of admitted VAs; and

(ii) confirming that the policies and procedures for admitting (eg, token admission criteria), halting, suspending and withdrawing VAs as well as for the ongoing monitoring of the admitted VAs will comply with relevant regulatory requirements.

2.3 *Part C – Custody of VA*

(i) explaining the proposed wallet structure and systems, wallet management policies and governance procedures and operational flow of VA transfer between different wallets;

(ii) confirming that client assets will be protected in a way comparable to the standards expected of traditional financial institutions. In particular, the report should confirm that:

(a) effective controls will be in place to ensure 98% of client VA will be stored in cold storage;

(b) there will be detailed specifications and proven processes for how access to cryptographic devices or applications will be authorised and validated, covering key generation, distribution, storage, use and destruction, and how a signatory's access could be immediately revoked as required;

(c) there will be a detailed mechanism with sufficient checks and balances and controls for transfer of VA between hot, cold and other storages, and the scope of authority of each function designated to perform any non-automated process in such transfer will be clearly specified; and

(d) there will be robust procedures to deal with events such as hard forks or airdrops from an operational and technical point of view;

(iii) confirming that there are sufficient controls and governance procedures for private key management to ensure all cryptographic seeds and private keys will be securely generated, stored and backed up in Hong Kong. In particular, the above should provide that:

(a) the generated seeds and private keys will be sufficiently resistant to speculation or collusion, and the manner in which the seeds and private keys are generated will ensure true randomness and thus will not be reproducible;

(b) access to seeds and private keys relating to client VA will be tightly restricted among authorised personnel, and no single personnel of the platform operator will have possession of information on the entirety of the seeds, private keys or backup passphrases, and controls will be established and implemented to mitigate the risk of collusion among authorised personnel of the platform operator;

(c) access control to backups of seeds or private keys will be stringent, and will be kept and distributed in a manner which mitigates any single point of failure and ensures that they cannot be re-generated based solely on the backups stored in the same physical location; and

(d) seeds and private keys will be stored in Hong Kong;

(iv) providing an assessment of the storage method to be implemented by the platform operator to store client VA (taking into account the new developments in security threats, technology and market conditions), and confirming that the wallet storage technology will be fully tested before deployment to ensure reliability;

(v) confirming that there will be adequate processes in place for safe handling of deposit and withdrawal requests for client VA to guard against risks involved in the process (eg, loss arising from theft, fraud and other dishonest acts, professional misconduct or omissions), in particular, confirming that:

(a) there are clear processes in place to evaluate the potential impact and risks of these developments as well as for handling fraud attempts specific to distributed ledger technology;

(b) there is a mechanism in place to check and monitor client IP addresses and whitelist client wallet addresses used for deposit and withdrawal by using appropriate confirmation methods;

(c) policies and procedures are in place to ensure any decision to suspend the withdrawal of client VAs will be made on a transparent and fair basis, and the platform operator will inform the SFC and all its clients without delay; and

(d) there will be processes in place to guard against fraudulent requests or requests made under duress, or controls to prevent personnel of the platform operator from transferring assets to wallet addresses other than the whitelisted addresses; and

(vi) confirming that there is a robust process to prepare, review and approve reconciliations of client assets in a timely and efficient manner, reconciliations will be checked and reviewed by appropriate staff members, and material discrepancies and long outstanding differences will be escalated to senior management on a timely basis for appropriate action.

2.4 *Part D – Know-your-clients (KYC)*

(i) explaining the proposed KYC policies and procedures (including any technologies to be deployed in the process), and explaining the operational flow that illustrates different stages in the KYC process (including identification and verification, signing of client agreement, disclosure to clients, data collection and usage, escalation/reporting, etc);

(ii) confirming that the proposed KYC policies and procedures fall within the acceptable account opening approaches under the relevant regulatory requirements;

(iii) confirming that a comprehensive pre-implementation assessment covering the required scope has been performed by qualified and independent external assessor to evaluate the appropriateness and effectiveness of the adopted processes and technologies for remote onboarding of overseas individual clients;

(iv) confirming the effectiveness of KYC process in establishing the true and full identity of clients, financial situation, source of funds/wealth, investment experience and investment objectives;

(v) confirming that there is a process in place to assess the client's knowledge of VAs before providing any services to the client, and to handle clients which do not possess such knowledge;

(vi) confirming that there is a process in place to assess the client's risk tolerance level and risk profile and determine the risk profile and assess whether it is suitable for the client to participate in the trading of VAs; and

(vii) confirming that there is a process in place to set a limit for each client to ensure that the client's exposure to VAs is reasonable, as determined by the platform operator, with reference to the client's financial situation and personal circumstances.

2.5 *Part E – Anti-money laundering and counter-financing of terrorism (AML/CFT)*

(i) explaining the proposed AML/CFT policies, procedures and controls (AML/CFT systems);

(ii) confirming that the proposed AML/CFT systems are adequate and appropriate to manage and mitigate the money-laundering and terrorist-financing (ML/TF) risks and ensure compliance with the regulatory requirements, in particular, confirming that there are adequate and appropriate AML/CFT systems in place to comply with the requirements on:

(a) customer due diligence measures (including simplified due diligence and determination of jurisdictional equivalence; all specific requirements covering high risk situations, customer that is not physically present for identification purposes and politically exposed persons; requirements for obtaining additional customer information as appropriate; and additional due diligence measures for cross-border correspondent relationships);

(b) ongoing monitoring (including screening of VA transactions and associated wallet addresses and monitoring of additional customer information);

(c) VA transfers when the platform operator conducts VA transfers and/or acts as an ordering institution, an intermediary institution or a beneficiary institution, and related sanctions screening requirements; and

(d) third-party deposits and payments (including ascertaining the customer's ownership or control of the account maintained with the ordering or beneficiary institution, or the unhosted wallet); and

(iii) confirming that the proposed AML/CFT systems would enable the platform operator to:

(a) adopt a risk-based approach having due regard to the regulatory requirements (eg, the list of non-exhaustive illustrative risk indicators for assessing ML/TF risks) when conducting institutional risk assessment and customer risk assessment; and

(b) identify suspicious transactions and activities having due regard to the list of non-exhaustive illustrative indicators of suspicious transactions and activities.

2.6 *Part F – Market surveillance*

(i) explaining and confirming that there are policies and controls for surveillance of the VA trading platform to identify, prevent and report any market manipulative or abusive trading activities;

(ii) confirming the types of trading activities identified and monitored by the platform operators have covered a majority of the manipulative or abusive trading activities that may potentially arise in relation to its scope of business and activities;

(iii) explaining the setting, types of parameters and alerts, related thresholds, methodology and operations of the proposed external surveillance system and how the system is being adapted and deployed for identifying, detecting and preventing any market manipulative or abusive trading activities; and

(iv) explaining any testing conducted on the proposed external surveillance system and confirming the efficacy of the proposed external surveillance system for identifying, detecting and preventing any market manipulative or abusive trading activities.

2.7 *Part G – Risk management*

(i) explaining and confirming that there are appropriate and effective policies and procedures which enable the platform operator to identify, measure, monitor and manage the risks, whether financial or otherwise, to which the platform operator, its associated entity and its clients are exposed, including but not limited to counterparty risk, market risk, credit risk, financial risk and operational risk;

(ii) explaining and confirming that there is an effective and independent risk management function, together with the senior management of the platform operator, which defines risk policies, establishes and maintains risk measures, monitors and regularly reviews risk management policies and procedures;

(iii) explaining and confirming that there are risk management and supervisory controls for the operations of the VA trading platform, for instance, system controls (eg, to prevent “fat finger” errors and acceptance of orders, to cancel orders), automated pre-trade controls and post-trade monitoring.

2.8 *Part H – Cybersecurity*

(i) identifying cybersecurity risks (including risk of fraud, errors and omissions, interruptions or other operational or control failures);

(ii) explaining and confirming the adequacy of proposed IT budget and the comprehensiveness of proposed IT inventory list for implementation and operations of the planned IT infrastructure, systems and security controls supporting the business activities and operations;

(iii) confirming the planned IT infrastructure and systems are in compliance with relevant requirements and sound industry practices, and can achieve a high level of information security, system resilience and business continuity;

(iv) confirming that there are policies and procedures to effectively manage and adequately supervise the design, development, deployment and operations of the VA trading platform, which includes its trading system and custody infrastructure, and the platform operator will regularly review the same in line with changing market and regulatory developments;

(v) confirming that the platform operator will assign adequately qualified staff, expertise, technology and financial resources to the design, development, deployment and operations of the VA trading platform;

(vi) confirming that the platform operator will perform appropriate due diligence, conduct ongoing monitoring and make appropriate arrangements regarding any third-party service provider to ensure that it will comply with the applicable legal and regulatory requirements;

(vii) confirming that there are written standard operating procedures (SOP) for performing system upgrades and maintenance, which contain, among other things, (a) the methods of communication, as well as how pending orders still in the order book are dealt with; (b) information on how long orders can be entered, amended or cancelled after a system downtime, and before continuous trading resumes; and (c) the process applicable to unexpected and unplanned system failures which affect an orderly market;

(viii) confirming that there are policies and procedures to ensure that the trading system and all modifications to the system will be tested before deployment and will be regularly reviewed, and a clear audit trail will be maintained for all modifications made to the trading system;

(ix) confirming that there are policies and procedures to inform the applicant's clients as far in advance as practicable if any trading system outages may affect them;

(x) confirming that the applicant will employ adequate, up-to-date and appropriate security controls to protect the VA trading platform from being abused, and the security controls should at least include (a) robust authentication methods and technology to ensure restricted access to the VA trading platform, (b) two-factor authentication for client logins, (c) effective policies and procedures for passwords, (d) stringent password policies and session timeout controls, (e) client notification for certain activities, (f) adequate security controls over infrastructure, (g) up-to-date data encryption and secure transfer technology, (h) up-to-date security tools to detect, prevent and block any potential intrusion, security breach and cyberattack attempts; and (i) adequate internal procedures and training for the applicant's staff and regular alerts and educational materials for its clients to raise awareness of the importance of cybersecurity and the need to strictly observe security in connection with the system;

(xi) confirming that there are policies and procedures specifying how a suspected or actual cybersecurity incident will be escalated internally and externally;

(xii) confirming that there are policies and controls to (a) regularly monitor the usage capacity of the VA trading platform and develop the appropriate capacity planning; (b) regularly stress-test the capacity of the VA trading platform to establish system behaviour under different simulated market conditions, and document the results of the stress tests and any actions taken to address the findings of the stress tests; (c) ensure there will be sufficient capacity to handle any foreseeable increase in the business volume and market turnover; and (d) there will be contingency arrangements, the details of which have been communicated to clients;

(xiii) confirming there is a contingency plan in place to cope with emergencies and disruptions related to the VA trading platform, including checking and ensuring data integrity after system recovery and ensuring that trading can be conducted in a fair and orderly manner after resumption; and

(xiv) confirming that there are policies and procedures to ensure backup facility and the contingency plan will be reviewed, updated and tested for viability and adequacy at least on a yearly basis.

SFC 證監會

Appendix 2

Second-phase Assessment – assessment on implementation effectiveness

Format of assessment report

1. The assessment report should cover the following items:

- Executive summary
- Expertise, experience and track record of the external assessor(s)
- Scope/areas of the assessment
- Limitation of the assessment
- Approach to the assessment
- Description of the specific areas that have been assessed and the approach and assessment procedures carried out by the external assessor(s)
- Clearly set out and explain any deviation from the plan and assess whether such deviation result in non-compliance with the applicable legal and regulatory requirements
- Detailed findings and recommendations on areas that are not deployed or implemented properly or as planned and the actions taken by the platform operator to rectify the matters

Areas to be covered

2. The SFC expects the Second-phase Assessment to assess whether the policies, procedures, systems and controls of at least the following areas are properly implemented (as mentioned in First-phase Assessment), tested or sample checked and, where applicable, have backup. Any deviation from the planned policies and procedures must be clearly set out and explained.

2.1 *Part A – Token admission*

- VAs proposed to be admitted for trading
- token admission and review committee

2.2 *Part B – Custody of VA*

- wallet systems and backup
- wallet operating systems
- vault room and other storage

- key rotation
- backups of seeds or private keys
- access and controls to seeds and private keys and the backups
- internal hot-to-cold and cold-to-hot transfer, rebalancing and replenishment
- handling of client deposit and withdrawal request
- whitelisting of wallet addresses for deposit and withdrawal
- reconciliation of client assets

2.3 *Part C – KYC*

- client onboarding process
- professional investor assessment
- client VA knowledge test
- client risk tolerance level assessment
- client risk profiling
- setting of exposure limit
- client agreement and terms and conditions
- disclosure to clients

2.4 *Part D – AML/CFT*

- institutional risk assessment
- customer risk assessment
- customer due diligence measures
- simplified due diligence and determination of jurisdictional equivalence
- all special requirements covering high risk situations, customer that is not physically present for identification purposes and politically exposed persons
- additional due diligence measures for cross-border correspondent relationships
- keeping customer information up to date

- transaction monitoring
- sanctions screening
- suspicious transaction reporting
- VA transfers
- third-party deposits and payments

2.5 *Part E – Market surveillance*

- setting of alert types, parameters and thresholds
- back-testing and sample check of the alerts / cases generated
- review and assessment of alerts / cases generated
- ongoing review (eg, management reports, trend analysis)

2.6 *Part F – Trading system and risk management*

- trading system and matching engine
- system controls
- pre-trade controls
- login monitoring
- pre-fund monitoring
- staff access control to trading information
- API
- failover and contingency drill for unexpected and unplanned outage

2.7 *Part G – Cybersecurity*

- IT system and control tests have been conducted so that there would be a high level of assurance of smooth operation, information security, system resilience and business continuity.

  (a) platform reliability

  (b) platform security

  (c) platform capacity and stress testing (including capacity of the VA trading platform)

  (d) system and data backup

(e) data integrity and confidentiality

(f) user access management

(g) patch management

(h) end-point protection

(i) unauthorised installation of hardware and software

(j) contingency

- The Second-phase Assessment should also cover the following:

  (a) check and confirm all external service providers (eg, market surveillance tools, AML/CFT tools, KYC tools) have been engaged and the relevant systems provided by them are fully adapted as planned and are in operation.

  (b) perform vulnerability assessment to identify, rank and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system. The report should list out potential risks posed by known vulnerabilities ranked in accordance with risk level. The vulnerability assessment should cover external and internal vulnerability scan.

  (c) perform penetration tests on network devices, firewalls, servers, databases, wallets and web applications. Testing must include both application layer and network layer assessments. The report should describe each vulnerability verified and/or potential issues discovered.

  (d) confirm that the major/critical rectification steps have been taken for all medium to high risk items identified in the penetration and vulnerability tests.