Scope of External Assessment Reports

June 2023

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 Licensed3n-i2 Corporations and SFC-licensed VA Service Providers). Please refer
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,

Appendix 1

First-phase Assessment – assessment on design effectiveness

Format of assessment report

1. The assessment report should cover the following items:

   - Executive summary
   -

with supervisory and reporting responsibilities assigned to appropriate staff members;

(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

(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.

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.