Regulatory Sandbox Exemptions

Guidelines for Applicants

FINANCIAL SERVICES AUTHORITY

Bois De Rose Avenue
P.O. Box 991
Victoria
Mahé
Seychelles

Tel: +248 4380800
Fax: +248 4380888
Website: www.fsaseychelles.sc
Email: enquiries@fsaseychelles.sc

Version: 31st December, 2019

Table of Contents

1. Introduction 4
   1.1. Enquiries 4
2. Scope of the Guidelines 4
3. Expectations of the Authority 5
4. Sandbox Application Process 5
   4.1. Queries in Regards to Application 5
   4.2. Application Form Components and Required Supporting Documents 6
   4.3. Application Submission 6
   4.4. Administrative Processes of Applications 6
   4.5. Incomplete Submission 7
   4.6. Meeting / Call with the Applicant 7
   4.7. Notification of Decision on Application 7
   4.8. Exit Strategy 8
5. Service Standards 8
6. The Fee 8
7. Auditor 9
8. Sandbox Preparation Process 9
   8.1. Key Preparation Stage Review Attributes 10
      8.1.1 Integrity of the Applicant and Key Persons 10
      8.1.2 Financial Capability and Professional Indemnity Insurance 11
      8.1.3 Key Risks and Mitigating Actions 11
      8.1.4 Client Safeguard Measures 12
9. Submission of Testing Parameters, Client Safeguards and Risk Management Measures 12
   9.1. Required Components of Testing Parameters and Test Cases 12
   9.2. Required Components of Client Safeguard Measures 13
   9.3. Required Components of Risk Management Measures 14
   9.4. Administrative Processes of Preparation Components 16
10. Sandbox Testing Period 16
   10.1. Changes to Applicant Information 17
   10.2. Regular Report 17
      10.2.1 Regular Report Components 17
      10.2.2 Report Submission 18
      10.2.3 Administrative Processes of Regular Report 18
   10.3. Mitigation Plan 19
      10.3.1 Mitigation Plan Components 19
      10.3.2 Mitigation Plan Submission 19
      10.3.3 Administrative Processes of Mitigation Plan 20
   10.4. Cessation Notice 20
      10.4.1 Response to Cessation Notice Components 20
      10.4.2 Submission of Response to Cessation Notice 20
      10.4.3 Administrative Processes of Response to Cessation Notice 21
   10.5. Extension Request 21
      10.5.1 Required Components of Extension Request 21
      10.5.2 Extension Request Submission 22
      10.5.3 Administrative Processes of Extension Request 22

11. Sandbox Exit 22
11.1. Outcomes of the Sandbox 22
11.2. Initiation of Exit from the Sandbox 22
11.2.1 Transition to formal licensing 22
11.2.2 Product and service termination 23
11.2.3 Forced exit 23
11.3. Applicant Notification Responsibilities to its Clients 24
11.4. Discontinued Service 24
11.4.1 Exit Plan Components 24
11.4.2 Exit Plan Submission 25
11.4.3 Administrative Processes of Exit Plan 25
11.4.4 Third Party Confirmation 26
11.4.5 Closure Report for Discontinued Service 26
11.5. Transition to Formal Licensing / Deployment 27
11.5.1 Intended Transition to License 27
11.5.2 Transition Plan Components 27
11.5.3 Transition Plan Submission 28
11.5.4 Administrative Processes of Transition Plan 28
11.5.5 Third Party Confirmation 29
11.5.6 Closure Report for Discontinued Service 29
12. Communication Protocol 30
13. Role of the Authority 30
Appendix 1 32
Appendix 2 34

1. Introduction

These guidelines have been prepared by the Financial Services Authority ("the Authority") to provide guidance on matters pertaining to the Regulatory Sandbox applicants under the Financial Services Authority (Regulatory Sandbox Exemption) Regulations, 2019 ("the Regulations").

The regulatory sandbox ("sandbox") allows firms to test innovative eligible financial services or products within a defined duration and controlled environment. It shall include adequate safeguards measures to ensure consumer protection in cases of failure and to ensure the overall safety and soundness of the financial system.

The sandbox allows for testing through exemptions from certain licensing, disclosure and reporting requirements under the Securities Act, 2007 on a case-by-case basis.

These guidelines explain the roles and responsibilities of the applicant, as well as provide guidance on the procedures for applying and operating within the Regulatory Sandbox.

1.1 Enquiries

Enquiries on application related matters should be forwarded to the Authority:

By Post: The Chief Executive Officer
Financial Services Authority
P.O. Box 991
Bois De Rose, Mahé
Republic of Seychelles

Attn: Capital Markets and Collective Investment Schemes Supervision Section

By e-mail: enquiries@fsaseychelles.sc

Tel: +248 4 380 800
Fax: +248 4 380 888

2. Scope of the Guidelines

The scope of this document is the Regulatory Sandbox Exemptions Guidelines for applicants to the Regulatory Sandbox implemented by Capital Markets and Collective Investment Supervision Schemes Section (CM&CISSS) of the Authority. The following Guidelines should be observed by applicants, in conjunction with the Financial Services Authority (Regulatory Sandbox Exemption) Regulations, 2019.

The Regulations and Guidelines applies to applicants providing eligible financial services, general insurance product, life risk insurance product or superannuation product, where:

"Eligible financial services" means:

(a) Providing financial product advice in relation to a particular kind of financial product
(b) Applying for or acquiring a particular kind of financial product
(c) Issuing, varying or disposing of a non-cash payment facility, or
(d) Arranging for the issuing, varying or disposing of a particular kind of financial product.

"Eligible general insurance product" means a general insurance product issued by an insurance company that is either authorised by the Authority or is a general insurance product authorised by the Authority for the purposes of these Regulations;

"Eligible life risk insurance product" means a life risk insurance product issued by an insurance company that is either authorised by the Authority or is a life risk insurance product authorised by the Authority for the purposes of these Regulations;

"Eligible superannuation product" means a superannuation product offered from a jurisdiction that has the approval of the Authority for the purposes of these Regulations.

3. Expectations of the Authority

An applicant to the Regulatory Sandbox may obtain an exemption by:

(a) Completing a written application in the form and manner as specified by the Authority;
(b) Satisfying the requirements as set out in the First Schedule; and
(c) Complying with the conditions or restrictions imposed by or in accordance with these Regulations.

The Authority expects the applicant and key persons to have the integrity, competence and financial standing to conduct business in the Regulatory Sandbox:

(a) Integrity: The integrity of oversight staff establishes trust and thus provides the basis for reliance on their judgement.
(b) Competency: Oversight staff should apply the knowledge, skills, and experience required in the performance of oversight inspections.
(c) Financial standing: status that indicates a person is in good financial situation.

4. Sandbox Application Process

To be able to participate in the Regulatory Sandbox in Seychelles, application and approval for the exemption from the Authority is obligatory.

4.1 Queries in Regards to Application

In the event that the applicant has queries prior to the application, a query may be submitted to the Authority via email or letter. The email and address details are provided in the first section of these Guidelines and on the Authority website.

The applicant should note that the query may be recorded by the Authority, in order to support the development of a Frequently Asked Questions ("FAQ") guide. Once the FAQ guide is developed, the applicant should refer queries to the FAQ guide first, then make further inquiries to the Authority in the event that the FAQ guide does not provide sufficient detail.

4.2 Application Form Components and Required Supporting Documents

All application forms and other documents are available from the Authority's website (www.fsaseychelles.sc).

The applicant must fill out the application form in accordance with the instructions detailed on the form, and complete the checklist attached to the form.

The applicant should ensure that the application form contains the following components, along with all the relevant attachments as specified in the application form:

(a) Company information;
(b) Application fee of USD5000;
(c) Business plan (if applicable);
(d) Risk Management (if applicable);
(e) Corporate governance structure of the applicant (if applicable);
(f) Organization structure of the applicant (if applicable);
(g) Certified copy of current valid license or other authorization or registered certification to conduct such business under the laws of a recognized jurisdiction if the applicant is operating outside Seychelles (if applicable); and
(h) Exit strategy/plan (if applicable).

4.3 Application Submission

The application form should be filled out in full, and the required supporting documents should be obtained by the applicant and key persons prior to submission.

By Mail

The applicant is to submit the physical form by mail, the application form should be mailed to the Authority in accordance with the instructions provided on the application form, and be submitted alongside all required supporting documents. The address and further details for submission are provided on the application form.

Note that a person who supplies, to the Authority, information in connection with an application which he knows ***or reasonably knows is false or misleading, is guilty of an offence, and enforcement/ proper action would be taken in line with FSA Act and Securities Act.***

4.4 Administrative Processes of Applications

Following submission of the application form, the Authority will initiate the review and processing of a complete application. The following steps will be carried out:

Step 1: Acknowledge the receipt of the application pack within 1 working day; assign a case number to the applicant and provide details of the designated contact person ("Case Officer") to the applicant. The applicant will receive all relevant information via the Sandbox mailbox (Regulatory.Sandbox@fsaseychelles.sc) . The applicant should direct all queries, communications and submission of documents to their designated Case Officer.

Step 2: Carry out an initial review of the application to assess whether the application is complete according to the requirements detailed herein.

Step 3: Begin to process the application if the application is deemed to be complete; or return the application to the applicant if the application is deemed to be incomplete, highlighting the area(s) of deficiencies. Please note that the Authority may provide general and brief guidance on the area(s) of deficiencies, but it is the responsibility of the applicant to engage suitable professionals or service providers to ensure the completeness of the application.

Step 4: Request for additional information or supporting documents for consideration of the application from the applicant, if necessary. The applicant is required to provide any additional information and supporting documentation within the agreed upon timeframe, and via the appropriate method (e.g. provision of physical documents or online copies).

Step 5: The FSA will communicate to the applicant regarding whether the proposed service(s) or product(s)is being considered or not. Should the application be considered, the FSA will advise on the way forward with respect to the Preparation stage.

4.5 Incomplete Submission

The application may be deemed incomplete if the applicant has not:

(a) Completed the application form in full or to an adequate degree; or
(b) Provided the required relevant documents, references, verifications or declarations to support the application in full.

The Case Officer will notify the applicant following review of the application to detail issues or request for further information or documentations. The applicant should respond to the notification at the earliest possible date. Applicants will have a period of 1 month for resubmission of the application. If the completed application form and relevant supporting documentation have not been re-submitted to the Authority within 1 month of the notification, the application will be considered as void and a new application would have to be lodged along with payment of the required application fee, should the applicant remain interested in proceeding further with the application. The applicant will be informed of the Authority's decision via the Sandbox mailbox, as well as through letter.

4.6 Meeting / Call with the Applicant

The Case Officer, a Supervisor and the Director of Capital Markets may hold a meeting / call with the applicant during the application review process described in Section 4.4.

The purpose of the meeting could be to understand further details about the applicant's proposed product / service, discuss areas requiring further clarification and gauge the applicant's ability to launch the product / service.

4.7 Notification of Decision on Application

The Case Officer will notify the applicant on FSA's decision on whether the proposed service(s) or product(s)is being considered or not. Should same be considered under the sandbox, the application moves to the preparation stage.

If the application is declined, the applicant may appeal the decision by following the Appeal Board's process.

4.8 Exit Strategy

The applicant should ensure that there is an exit strategy in place that could be implemented in the event of product / service testing termination due to business performance, breaches, transition to license or other reasons. The exit plan should contain the following components:

(a) Length of time the applicant would require to unwind product / service;
(b) Timeline and protocol for notification to clients;
(c) Timeline for return of client's assets;
(d) Potential impact to other stakeholders.

If the exit plan is not appropriate, the Case Officer will discuss further with the applicant, and require the applicant to provide a revised exit plan. If after 1 month following the discussion, no response is received or no agreement is reached upon discussion, the Case Officer will reject the application and write to inform the applicant accordingly.

5. Service Standards

The Authority's current Service Standards for processing the application for Regulatory Sandbox exemptions, from receipt of a completed application for consideration by the Authority, is thirty (30) working days.

It is important to note that this service standard will only be achievable if all the requisite information / documents are provided at the time the application is lodged. The Authority is not responsible for delays arising from the submission of incomplete applications. The following is to be further noted:

The Authority will only process complete applications. Incomplete applications exceeding the resubmission timeframe will be considered as void and a new application would have to be lodged along with payment of the required application fee.

This document is not exhaustive or binding on the Authority. The exemption regime requires the Authority to exercise discretion. How the Authority does this will depend on the applicant's particular circumstances.

6. The Fee

The fee will be determined based on the structure and Guidelines outlined in the Financial Services Authority (Regulatory Sandbox Exemption) Regulations, 2019.

The applicant submits a written application and application fee (USD 5,000) to the Authority. After a final decision is provided for providing an eligible financial services the applicant shall pay the exemption fee.

For the first 12 months or part thereof of the testing period:

(a) USD4,000 for providing financial product advice in relation to a particular kind of financial product;
(b) USD4,000 for applying for or acquiring a particular kind of financial product;
(c) USD5,000 for issuing, varying or disposing of a non-cash payment facility; and
(d) USD10,000 for arranging the issuing, varying or disposing of a particular kind of financial product.

For the second 12 months or part thereof of the testing period the fee shall be dependent on the nature and complexity of the financial product; but shall not exceed 150% of the exemption fee payable based on the item above.

The total fee will be communicated to the applicant by the Case Officer following the submission and review of the application form.

The applicant should provide a cheque with the correct amount, made payable to the Authority.

In the event that the fee is not correct or the cheque has not been completed properly, the Authority will return the cheque to the applicant and notify the applicant of the issue(s) with the fee or cheque. The applicant should then issue the correct cheque at the earliest possible date. If the cheque has not been submitted 1 month since the notification of the error, the application will be rejected.

If the fee is calculated correctly and the cheque has been banked, the Case Officer will notify the applicant regarding the confirmation of payment.

7. Auditor

The applicant should ensure that the auditor has the necessary qualifications and competencies to perform the audit of the financial statements for the proposed Regulatory Sandbox participant.

If the Authority deems the auditor not competent, the applicant will be required to change their auditor. If the applicant objects, the Case Officer will consider the grounds for the objection and review the decision.

8. Sandbox Preparation Process

The objective of the preparation stage is for the Case Officers to work with the applicant to agree the testing parameters, the client safeguards, risk management measures and undertake the relevant due diligence procedure.

The applicant should check that the following attachments have been submitted for the preparation process:

(a) Certified copy of current valid license or other authorization to conduct such;
(b) business under the laws of a recognized jurisdiction if the applicant is operating outside Seychelles (if applicable);
(c) Personal questionnaire ("PQ") along with all the attachments as requested in the PQ for directors, managerial staff, etc;
(d) Questionnaire for shareholders and BO along with all the attachments;
(e) Funding information and financials for the past 3 years;
(f) Current regulatory regime governing the applicant;
(g) Summary of the key risks and mitigations associated with the proposed product / service;
(h) Summary of the client safeguard measures;
(i) List of exemptions being requested;
(j) The Memorandum and Articles of Association;
(k) Procedures Manual;

(l) Compliance Manual;
(m) Anti-Money Laundering manual;
(n) Planned test cases and testing parameters; and
(o) Detailed Exit strategy

For documents that require certification, the applicant should ensure that they have been properly certified by a person who is authorised to certify and that the certification has been done in a proper manner. This includes:

(i) Identification documents;
(ii) Proof of Address;
(iii) Academic and professional qualifications etc.

A non-exhaustive list of due diligence requirements and list of constitutional documents are included in Appendix A and Appendix B of these Guidelines.

8.1 Key Preparation Stage Review Attributes

Following submission of the application form and supporting documents, the application will undergo a review by the Authority. The Authority will assess the following key attributes of the application:

8.1.1 Integrity of the Applicant and Key Persons

The Authority will review and determine the integrity of the applicant and its key personnel (e.g. directors, key management personnel, shareholders and beneficial owners). A key person is a director (or other person acting in the role of director), controller (any person with a direct or indirect interest of 10% or more of the shares in the applicant or who, in the opinion of the Authority has the ability to influence the applicant, the CEO, the compliance officer and any person who provides advice to or investment management for, a client.

The Authority may conduct further checking with relevant regulatory authorities, investigating bodies, banks, or other entities (e.g. Police, FIU, SRC, Central bank of Seychelles) in order to determine the integrity of the applicant. The Authority will make inquiries on the integrity, competence and financial standings of key persons via third party confirmations or request further information from the relevant persons.

The Authority requirements on key persons will be as follows:

(a) Key persons who are to be officers need to demonstrate sufficient experience and qualifications, which will be reviewed by the Authority;
(b) Key persons who have been disqualified from acting as a director of a company would not normally be acceptable;
(c) A key person who has been convicted of an offence involving dishonesty within the last ten years would not normally be acceptable. A key person who has been subject to investigation for an offence involving dishonesty should be invited to explain to the Authority the circumstances of the investigation and to convince the Authority that the investigation does not cast doubt on integrity.
(d) An undischarged bankrupt would not normally be acceptable as a key person. A person whose bankruptcy was discharged more than five years previously would normally be accepted

In the event that the Authority requests further documentation, clarifications or certifications from the key persons throughout the course of the case review, the applicant should provide a response and the required documentation to the Authority following the request notification. In the event that there are extenuating circumstances, the applicant should communicate the conditions to the Authority and discuss next steps with the Case Officer.

If the applicant does not respond within the 1 month latest of the initial request notification, and in the absence of extenuating circumstances, the Case Officer will write to notify that the application has been rejected via the Sandbox mailbox, as well as through letter.

Where a key person has been found to have concealed relevant information from the Authority or has made a statement that is false or misleading, the Case Officer will invite the key person to comment. Unless the Case Officer is satisfied that the error was a genuine mistake, the key person will not be accepted.

The applicant is able to challenge the Authority's view that key persons, shareholders, beneficial owners or independent directors are not acceptable, and may discuss further with the Case Officer to further review. However, the Authority reserves the right to make all final decisions on the integrity of the applicant and key personnel.

8.1.2 Financial Capability and Professional Indemnity Insurance

The professional indemnity insurance ("PII") cover is required by the Regulatory Sandbox exemptions framework. PII is intended to provide cover for a liability caused as result of an act of negligence of a Director / Officer / Employee. During the application stage, a quote for the PII will suffice; however, the applicant needs to submit proof of policy after approval in principle is received at the end of the application stage and before approval is received at the end of the preparation stage.

In the case of an existing company, an applicant's financial statements will be reviewed. In the case of start-ups or new companies that do not have audited financial statements, Case Officers will check sources of funding, level of funding, funding commitments, and forward looking forecasts. If the applicant does not have adequate capital, the applicant will be informed and invited to review its financial capability.

In the case where the applicant cannot find sufficient resources or does not respond within 1 month of notification, the Case Officer will reject the application and inform the applicant accordingly in writing.

8.1.3 Key Risks and Mitigating Actions

The applicant should detail the corporate governance structure, and should identify how risks are overseen. The applicant should consider risk areas (where applicable to their proposed product / service) such as but not limited to:

(a) Credit risk, market risk, liquidity risk, operational risk, reputation risk
(b) Client on-boarding and on-going monitoring
(c) AML / CTF / KYC controls
(d) Cybersecurity
(e) Capital requirements
(f) Prevention of Market Manipulative and Abusive Activities

The applicant should also identify higher level risks or mitigations.

8.1.4 Client Safeguard Measures

The applicant should identify safeguard measures such as but not limited to the following, where applicable to their proposed product / service:

(a) Data privacy controls
(b) Client money and assets protection
(c) Client risk profile
(d) Prevention of conflicts of interest
(e) Notifications to clients
(f) Dispute resolution mechanism

9. Submission of Testing Parameters, Client Safeguards and Risk Management Measures

The applicant is required to submit the detailed testing parameters and test cases, client safeguard measures, and the risk management framework within 30 working days of receiving FSA decision with respect to the proposed application.

The components should be submitted to the Case Officer via the Sandbox mailbox.

If the applicant has not submitted any of the above components after 1 month of the deadline, the Case Officer will reject the application and inform the applicant accordingly in writing. If there are extenuating circumstances that hinder the applicant from submitting the above components in full before the deadline, they may notify the Authority. The Authority will then determine whether there are extenuating circumstances justifying giving further time to the applicant.

If all the components have been received, the Authority will begin reviewing the components.

9.1 Required Components of Testing Parameters and Test Cases

The applicant should propose testing parameters and test cases based on requirements set out in the Regulations and consideration of the following:

(a) **Number of clients**: the maximum number of clients that the applicant can have at any one point in time shall be determined on a case by case basis by the Authority. The applicant should detail or propose system-based controls to have in place to prevent on-boarding of no more than the maximum number of clients specified by the Authority. If no system controls exist and there are no plans to introduce system controls, the applicant should detail the manual controls in place.

(b) **Type of clients**: the applicant should target the appropriate client segment for the product. In particular, the applicant should consider the level of risk associated with the product / service and the extent of knowledge and expertise required of the client, then determine whether the product / service is appropriate for retail clients or should be restricted to wholesale clients.

(c) **Maximum exposure per client**: the applicant should follow the specifications as listed in the Exemptions Regulations in setting the maximum exposure limits per client.

(d) **Time to begin testing**: the applicant should detail what stage of development the proposed product / service is in. In general, a prototype should have been developed and the applicant should be ready to commence testing in a live environment following the end of the Preparation stage.

(e) **Proposed product / service performance in previous testing**: applicants should have already conducted laboratory testing before application to the Sandbox and submit the test cases and outcomes to the Case Officer to understand how the product has performed in a test environment without real clients.

(f) **Testing plan and proposed test cases**: the applicant should detail the proposed testing plan and test cases in terms of the viability and soundness of implementing the tests in the Sandbox.

(g) **Other parameters**: the applicant should identify and review any other relevant parameters that apply to the proposed product / service.

In the event that the testing parameters and test cases do not adhere to the aforementioned criteria, the applicant should provide reasons or justifications.

The applicant should consider the applicability of implementing bespoke parameters based on the proposed product / service, such as:

(a) Reducing the number of clients who can be on-boarded;
(b) Placing additional restrictions based on profile of retail clients (e.g. age, income);
(c) Specifying a required mix between retail and wholesale clients; or
(d) Adding limits on the volume of transactions.

9.2 Required Components of Client Safeguard Measures

The applicant should propose client safeguard measures based on requirements set out in the Regulations and consideration of the following:

(a) **Data privacy controls**: the applicant should identify the policies / procedures relating to data privacy and implementation of an adequate data privacy framework. This should cover but not be limited to:

  (i) Breach notification
  (ii) Right to access
  (iii) Privacy by design

(b) **Client moneys and assets protection**: the applicant should identify the policies / procedures relating to client moneys and asset protection and define an appropriate framework for handling of client's moneys and assets by intermediaries. This should include, for example, establishment of segregated accounts for client's moneys and assets and conducting transactions only in designated bank accounts in the client's name.

(c) **Client risk assessment mechanism**: the applicant should identify the policies / procedures relating to client on-boarding. Where the applicant is targeting retail clients, should provide a mechanism to assess the clients' risk profile and to use this to ensure that the products / services offered to the client are suitable for their needs.

(d) **Prevention of conflicts of interest**: the applicant identifies the policies / procedures relating to managing and preventing conflicts of interest. This should include policies and controls for identifying and mitigating potential conflicts. For example, applicants proposing products / services relating to the trading of securities should establish policies and procedures governing employees' dealings in securities to eliminate, avoid, manage, or disclose actual or potential conflicts of interest.

(e) **Notifications to clients**: the applicant should provide client communications templates, which specifies that the applicant is operating under an exemption and provides full disclosure of the potential risks and any available compensation arrangements.

(f) **Dispute resolution mechanism**: the applicant should provide details of a dispute resolution mechanism through which clients can raise issues with the product / service. This may include, for example, professional indemnity insurance.

(g) **Other client safeguard measures**: Identify and review any other measures that apply to the proposed product / service.

The applicant should consider the applicability of implementing bespoke client safeguard measures based on the proposed product / service, such as:

Examples of bespoke client safeguard measures are:

(a) Specifying additional transaction limits;
(b) Increasing the frequency or type of notification to clients;
(c) Requiring secondary checks by a financial advisor for advice provided by robo-advisory services.

Examples of bespoke client safeguard measures for crypto exchanges are:

(a) Capital requirements mandating exchanges to maintain sufficient capital buffer to provide a higher chance of recovery;
(b) Insurance policy for theft or hacking;
(c) Assessment of client's knowledge of virtual assets and the associated risks;
(d) Publishing trading rules on the website.

9.3 Required Components of Risk Management Measures

The applicant should design and outline risk management measures based on requirements set out in the Regulations and consideration of the following:

(a) **Risk management policy**: the applicant should identify the policies / procedures relating to risk management, clearly outlining the following information:

(i) Risk governance structure
(ii) Risk appetite statement

(iii) Risk categories used by the organization
(iv) Approach to the identification, assessment, management, monitoring and reporting of risks
(v) Roles and responsibilities for risk
(vi) Approach to management and escalation of breaches

(b) **Risk register**: the applicant should detail the risk register for the product / service, identify relevant risks for the product and propose mitigations. This should include but not limited to the following:

(i) Credit risk
(ii) Market risk
(iii) Liquidity risk
(iv) Operational risk
(v) Reputational risk

(c) **Client on-boarding and on-going monitoring**: the applicant should propose policies / procedures relating to client on-boarding and on-going monitoring. These policies and procedures should cover the following requirements and adhere to Seychelles Anti-Money Laundering Laws where applicable:

(i) Client due diligence and KYC compliance
(ii) AML / CFT compliance
(iii) Ongoing due diligence
(iv) Transaction monitoring
(v) Regulatory reporting

(d) **Cybersecurity**: the applicant should identify the policies / procedures relating to cybersecurity. The policies / procedures should outline the processes in place to identify, protect, detect, respond, and recover from cybersecurity threats.

(e) **Prevention of market manipulative and abusive activities**: The applicant should ensure the procedures relating to market manipulative and abusive activities provided at the application stage includes details of how the organization identifies, prevents, and reports malicious actors behind any market manipulative or abusive activities. The applicant should supplement relevant details to the procedures where necessary.

(f) **Other risk management components**: Identify and report to the Authority other relevant risk management components that apply to the proposed product / service.

The applicant should consider the applicability of implementing bespoke risk management measures based on the proposed product / service, such as:

Examples for bespoke risk management measures are:

(a) Setting limitations on the volume of lending for a P2P lender;
(b) Increasing the reserve ratio; or
(c) Requiring mitigations for additional risks, such as strategic risk, based on the business strategy.

Examples of bespoke risk management measures for crypto exchanges are:

(a) System checks for managing money laundering and terrorist financing risks;
(b) Due diligence on the virtual assets before listing;
(c) Limits on margin trading;
(d) Written policies and procedures on conflicts of interest and policies against regulatory violation;
(e) Additional policies and procedures on market manipulation and abusive activities;
(f) Maintenance of segregated accounts for client money and virtual assets in a designated trust account or client account and store sizable assets in cold storage;
(g) Additional reporting requirements.

9.4 Administrative Processes of Preparation Components

The Authority will initiate the review of testing parameters and test cases, client safeguard measures, risk management measures and review the relevant due diligence submitted by the applicant. The process of the review for each component will be as follows:

Step 1: Acknowledge receipt of the required component via the Sandbox mailbox.

Step 2: Carry out an initial review of the component to assess whether the component is acceptable and compliant according to the requirements detailed herein.

Step 3: Provide feedback to the applicant (if any). Feedback could include questions, clarifications sought, or comments around the adequacy and completeness of the parameters and test cases, client safeguard measures, or risk management measures. Additionally, the feedback could include the bespoke requirements applicable to the specific product / service.

Step 4: The Applicant is responsible for providing a revised component to the Authority for review, within the specified timeframe. The Authority will review the revised plan for compliance and adequacy with the regulatory requirements.

Step 5: If the (revised) component is deemed satisfactory by the Authority, the Case Officer will inform the applicant about the approval to proceed to experimentation via the Sandbox mailbox, as well as through letter and request submission of the relevant exemption fee. If not, the Case Officer will return the application to the applicant for further discussion and review, or reject the application and inform the applicant accordingly via the Sandbox mailbox, as well as through letter.

Step 6: If the application is declined, the applicant may appeal the decision following the Appeal Board's process.

10. Sandbox Testing Period

If the application is approved, the applicant can begin testing of the proposed product / service in the Sandbox. The following section details the procedures, expectations and responsibilities of the applicant throughout the testing period.

10.1 Changes to Applicant Information

If there are any proposed changes to the applicant's corporate information, business strategy, proposed product or service, testing plan and test cases during the Sandbox testing period, the applicant shall seek approval from the Authority prior to implementing such changes.

The Authority will initiate the processing of the proposed changes upon submission of the supporting documents. The following steps will then be carried out:

Step 1: The Case Officer will acknowledge receipt of the update via Sandbox mailbox.

Step 2: The Authority will review the proposed change and undertake a completeness check on the documents provided, and repeat the procedures outlined in Sections 4 and 6. The Authority will consider the reputation, character, financial integrity and reliability of the proposed updates.

Step 3: The Case Officer may follow up with the applicant and undertake discussions where necessary to determine the impact of the changes and whether the changes are acceptable or not.

Step 4: The Authority will make a decision to accept or reject the applicant's changes, following discussions with the applicant. If the changes are deemed acceptable, the Case Officer will acknowledge the changes and inform the applicant of the decision. If the changes are not accepted, the Case Officer will follow up with the applicant to determine acceptable changes or measures the applicant should undertake in order to address concerns.

10.2 Regular Report

The applicant should submit reports in the manner and frequency as prescribe by the Authority to the Case Officer for the purposes of on-going supervision.

10.2.1 Regular Report Components

The applicant should ensure that the submitted report contains the following components, along with all the relevant attachments as specified in the application form:

(a) **Corporate information**: the applicant should state changes to corporate information as outlined in the application form (if any), in aspects such as:

(i) Corporate governance structure;
(ii) Ultimate beneficiaries' / board information;
(iii) Funding information and financials etc.

(b) **Description of business activities**: the applicant should state changes to the proposed business plan or proposed product / service within the Sandbox (if any), in aspects such as:

(i) Product / service descriptions;
(ii) Business strategy;
(iii) Documentation of key business activities;
(iv) Workflow and target operating model, etc.

(c) **Testing parameters**: the applicant should provide details and evidence of their compliance with the testing parameters throughout the Sandbox, as well as any changes undertaken.

(d) **Complaints register**: the applicant should submit a copy of the complaint register highlighting the complaints received, nature of complaints, status of the complaints and the service standard for each complaint.

(e) **Risk management measures**: the applicant should provide details and evidence of risk management measures implemented throughout the Sandbox, as well as any changes undertaken.

(f) **Client safeguard measures**: the applicant should provide details and evidence of the client safeguard measures implemented throughout the Sandbox, as well as any changes undertaken.

(g) **Testing outcomes**: the applicant should provide details on the outcomes of the testing plan and test cases.

(h) **Financial reports**: the applicant should provide financial reports of the product / service performance, along with an appropriate level of financial analysis. This could include aspects such as:

(i) Financial projections;
(ii) Profit and loss statements;
(iii) Liquidity and capital reporting, etc.

10.2.2 Report Submission

The frequency of report submission over the period of the Sandbox testing phase will be determined by the Authority following discussion with the applicant, and communicated to the applicant prior to the beginning of the testing period.

Submission of the report should be conducted through the dedicated Sandbox mailbox to the Case Officer.

If the applicant is unable to provide the required information/report within the agreed timeframe, the applicant should notify the Case Officer prior to the deadline. The Applicant should request for an extension providing valid explanations to the Case Officer. The Authority will communicate to the applicant the outcome of the request.

If the applicant fails to submit a complete report with all the required components within 1 month after the submission date, the Authority will decide whether to remove the applicant from the Sandbox and revoke the Exemptions given, and notify the applicant via the Sandbox mailbox as well as through letter.

10.2.3 Administrative Processes of Regular Report

If the applicant has submitted the report with all components required, the Authority will undertake internal review of the report. The process of the review for each component will be as follows:

Step 1: The Case Officer shall acknowledge receipt of the report.

Step 2: The Authority shall review the report to identify any breaches, gauge the severity of the breach, and propose further actions. Following the review, the Case Officer will notify the applicant of the review outcomes and next steps.

Step 3: If there are no breaches identified in the report, the Case Officer will write to the applicant and acknowledge the report via the Sandbox mailbox, and note any further actions required from the applicant.

Step 4: If a breach has been identified in the report, the Authority will assess the severity of the breach. If the breach is deemed not severe enough to warrant revocation of exemptions, the Case Officer will write to the applicant to notify that a breach has been identified, and request for a mitigation plan. If the breach is severe enough to warrant revocation of exemptions, the Case Officer will notify the applicant of the breach identified, and issue a cessation notice.

10.3 Mitigation Plan

The Authority will issue a request for mitigation plan and inform the applicant of:

(a) The list of breaches identified within the report review stage;
(b) Expected state of the applicant's testing parameters, outcomes, client safeguard and risk management measures, or controls; and
(c) Submission, review and monitoring timeframe.

10.3.1 Mitigation Plan Components

The applicant's mitigation plan should include, but not limited to, the following:

(a) Timeframe of implementation of mitigation plan;
(b) Details of mitigating actions and remediation actions to resolve and mitigate the breaches identified by the Authority;
(c) Changes to or implementation of additional testing parameters, client safeguard and risk management measures, controls, or other activities where applicable;
(d) Corresponding changes to policies and procedures, governance structure or roles and responsibilities of different parties as a result of implementation of the mitigation plan (if any);
(e) Viability of implementation of the mitigation plan, identification of any risks or impediments to implementation of the mitigation plan and steps to remove such impediments;
(f) Other components pertinent to demonstrating the soundness, viability and adequacy of the resolution of breaches identified.

10.3.2 Mitigation Plan Submission

Following the request, the applicant should investigate the breach and submit the mitigation plan within 10 business days of the request. If the applicant fails to submit a mitigation plan within the timeframe, the Authority will decide whether to revoke the applicant's exemptions.

10.3.3 Administrative Processes of Mitigation Plan

If the applicant has submitted the mitigation plan within the required timeframe, the Authority will undertake internal review of the plan. The process will be as follows:

Step 1: The Case Officer shall acknowledge receipt of the mitigation plan.

Step 2: The Authority will undertake internal review of the plan to determine whether the mitigation plan is acceptable or not.

Step 3: If the mitigation plan is deemed sound and acceptable, the Case Officer will notify the applicant of the acceptance of the mitigation plan and grace period extended to the applicant to implement the mitigation plan via the Sandbox mailbox. If the mitigation plan is deemed insufficient, the Case Officer will write and discuss further with the applicant. If no consensus on the mitigation plan can be reached between the Case Officer and the applicant, the Authority will revoke the applicant's exemptions and notify the applicant via the Sandbox mailbox as well as through letter.

10.4 Cessation Notice

The cessation notice acts as a final warning to the applicant to cease their current practices or activities which have caused a severe breach, and to implement remediation measures.

In the event that a breach has been identified which is severe enough to warrant exit, the Case Officer will issue a cessation notice via the dedicated Sandbox mailbox. The cessation notice will include:

(a) The identified breach that leads to the cessation notice.
(b) The Authority's expectations on a satisfactory response to the cessation notice.

10.4.1 Response to Cessation Notice Components

The applicant's response to the cessation notice should involve consideration of the following:

(a) Rationale and root causes for severe breach activities;
(b) Detailed mitigation plan and remediation actions to address and resolve the severe breaches identified by the Authority;
(c) Timeframe of implementation of mitigating actions and remediation activities;
(d) Corresponding changes or additions to testing parameters, client safeguards, risk management measures, controls, policies and procedures, governance structures, roles and responsibilities,
(e) Viability of implementation of the mitigation plan and remediation activities, identification of any risks or impediments related to implementation of such activities and plan to remove such impediments;
(f) Other components pertinent to demonstrating the soundness, viability and adequacy of the resolution of severe breaches identified.

10.4.2 Submission of Response to Cessation Notice

Submission of the cessation notice should be conducted through the dedicated Sandbox mailbox to the Case Officer.

Following the request, the applicant should investigate the breach and submit a response to the cessation notice within 10 business days of the issuance of the cessation notice. If the applicant fails to provide a response to the cessation notice within the timeframe, the Authority will revoke the applicant's exemptions.

10.4.3 Administrative Processes of Response to Cessation Notice

If the applicant has submitted the response to the cessation notice with all components required within the agreed timeframe, the Authority will undertake internal review of the response. The process of the review will be as follows:

Step 1: The Case Officer shall acknowledge receipt of the response.

Step 2: The Authority will undertake internal review of the response to determine whether the response to the cessation notice is acceptable or not.

Step 3: If the response is deemed sound and acceptable, the Case Officer will notify the applicant of the acceptance of the response and grace period extended to the applicant to implement the proposed mitigation plan or remediation activities as set out in the response. If the response is deemed insufficient, the Case Officer will write and discuss further with the applicant. If no consensus on the mitigation plan is reached between the Case Officer and the applicant, the Authority will revoke the applicant's exemptions and inform the applicant via the Sandbox mailbox, as well as through letter.

10.5 Extension Request

In cases that the applicant requires extension to the original length of Sandbox testing period, the applicant can apply for an extension request.

10.5.1 Required Components of Extension Request

The applicant's extension request should include the following information:

(a) Length of extension;
(b) Reasons for extension;
(c) Identification and documentation of changes as a result of the applicant's extension of the Sandbox testing phase, including potential changes to:

  (i) Business activities;
  (ii) Testing plan, test cases and testing outcomes;
  (iii) Financial performance;
  (iv) Client safeguard and risk management measures; and
  (v) Controls.

Proposed mitigation plans to address changes as a result of the extension, if the applicant anticipates that the changes could result in a breach or raise concerns with the Case Officer.

If the Case Officer or applicant identifies any other information as pertinent to the extension request, it should be discussed between the parties and included.

10.5.2 Extension Request Submission

Submission of the extension request should be conducted through the dedicated Sandbox mailbox to the Case Officer.

The applicant must submit the extension request at least 3 months prior to the end of their Sandbox testing period. If the applicant does not comply with this requirement due to extenuating circumstances, the applicant may notify the Case Officer of such reasons and await further review by the Authority.

10.5.3 Administrative Processes of Extension Request

If the applicant has submitted the extension request with all components required within the agreed upon timeframe, the Authority will undertake internal review of the request. The process of the review for the request will be as follows:

Step 1: The Case Officer shall acknowledge receipt of the request.

Step 2: The Authority shall review the request and decide if the request will be accepted. The Case Officer will notify the applicant of the decision via the dedicated Sandbox mailbox, as well as through letter.

11. Sandbox Exit

11.1 Outcomes of the Sandbox

Following the end of the Sandbox testing period for the applicant or the revocation of the exemptions, there are 2 outcomes for the applicant:

(a) Formal transition to licensing or deployment, meaning the applicant's business will undertake the formal licensing or deployment process to be launched outside of the Sandbox; or

(b) Discontinued service, meaning the termination of regulatory exemptions and cessation of the applicant's product or service.

11.2 Initiation of Exit from the Sandbox

There are 3 triggers that may lead to an exit from the Sandbox:

11.2.1 Transition to formal licensing

Following the end of the Sandbox testing period, the applicant should decide whether it intends to launch the product or service in the market and transition from Sandbox to formal licensing and deployment, via the dedicated Sandbox mailbox.

In the event that the applicant intends to transition to formal licensing and deployment outside of the Sandbox, the applicant is responsible for formally notifying the Case Officer 1 month prior to the end of the Sandbox testing period.

The Authority will undertake an internal review of whether to accept the applicant's request to transition to formal licensing.

The applicant shall provide details on the following aspects in order to facilitate the review process:

(a) Reasons behind the decision to transition to formal licensing;
(b) The applicant's testing outcomes and business performance during the Sandbox;
(c) Impact of deployment of the applicant's business to the market;
(d) Viability of implementing the applicant's business in the market;
(e) Potential impediments, risks, or issues in the deployment of the applicant's product or service in the market and methods to resolve

If the applicant's decision is accepted by the Authority, the Case Officer will inform the applicant accordingly via the dedicated Sandbox mailbox, as well as through letter. The applicant will begin proceedings to deploy its product / service and apply for a formal license. Further details on the initiation of the formal licensing phase is provided in Section 11.5 below.

If the applicant's decision to transition to formal licensing is not accepted by the Authority, the Case Officer will inform the applicant accordingly via the dedicated Sandbox mailbox, as well as through letter. The applicant will face discontinued service and begin proceedings to cease its Sandbox product / service, following procedures outlined in Section 11.4 in these Guidelines.

11.2.2 Product and service termination

In the event that the applicant reaches the end of the Sandbox testing period and does not pursue formal licensing or deployment, the applicant will face the end of regulatory exemption and product / service termination. The applicant is responsible for notifying the Case Officer 3 month prior to the end of the Sandbox testing period.

Product or service termination may be triggered due to the following reasons:

(a) The applicant reaching the end of its Sandbox testing period without request / approval for extension;
(b) The applicant requesting to discontinue testing the product or service during the testing phase;
(c) The applicant deciding not to pursue the product or service or having no intention to launch in market (e.g. due to poor performance), etc.

The Authority shall review and acknowledge the applicant's decision to undergo product and service termination. The Case Officer will provide acknowledgement of product / service termination via the dedicated Sandbox mailbox, as well as through letter, and notify the applicant that they will face discontinued service and begin proceedings to cease its Sandbox product / service, following the procedures outlined in Section 11.4 in these Guidelines.

11.2.3 Forced exit

Forced exit refers to a revocation of the applicant's Sandbox exemptions prior to the end of the Sandbox testing period, due to the following reasons:

(a) Severe breach identified during the Sandbox testing period;
(b) Inadequate, insufficient or lack of a sound mitigation plan or response to cessation notices;

(c) Issues throughout the Sandbox resulting in product or service termination such as lack or untimely response to the Authority's requests, untimely or incomplete submission of information and reports;
(d) Insolvency, bankruptcy or other factors that result in the cessation of the applicant's financial services product / service; or
(e) Any other issues that the Authority deems material.

The Authority reserves the right to make the final decision on whether the applicant's exemptions provided under the regulations should be revoked.

The Authority will undertake internal review of whether certain factors warrant a forced exit from the Sandbox. If the Authority decides to revoke the applicant's exemptions and remove them from the Sandbox, the Case Officer will inform the applicant accordingly via the dedicated Sandbox mailbox, as well as through letter. The applicant will face discontinued service and begin proceedings to cease its Sandbox product / service, following procedures outlined in Section 11.4 in these Guidelines.

11.3 Applicant Notification Responsibilities to its Clients

In the event of revocation of exemptions by the Authority, the applicant is responsible for notifying their clients in writing within 10 business days of exit triggered as a result of the following conditions, in accordance with the requirements set out in the Regulations:

(a) The eligible person has ceased to carry on a financial services business;
(b) The eligible person has become insolvent or has been the subject of insolvency, liquidation or administration proceedings, or any analogous procedures or steps, in any jurisdiction;
(c) The eligible person has become bankrupt or has applied to take the benefit of any law for the relief of bankruptcy or insolvent debtor or taken any analogous procedures or steps, in any jurisdiction;
(d) The eligible person has compounded with the creditors or has made an assignment of the remuneration for the benefit of the creditors;
(e) The eligible person has ceased to rely on the exemption provided under those regulations;
(f) The financial service or a financial product to which it relates, has materially changed;
(g) The financial service or a financial product to which it relates, is no longer being offered to new clients; or
(h) An event which may reasonably be considered to have a material effect on the client.

11.4 Discontinued Service

If the Authority has determined that the applicant will face discontinued service, an exit plan will be required. The objective of the exit plan is to facilitate the termination of the applicant's product or service in the Sandbox in a timely manner with minimal impact on its clients.

11.4.1 Exit Plan Components

The exit plan should be based upon the exit strategy as documented in the application pack. If there have been changes to the applicant's corporate information, business strategy, testing plan, test cases or other key factors of the applicant's product or service throughout the Sandbox period, the applicant should review and revise the exit strategy and exit plan accordingly. The applicant should then inform the Case Officer that there have been revisions to the exit plan and submit the revised plan for review.

The exit plan should include, at a minimum, the following components:

(a) Timeframe the applicant would require to unwind product / service;
(b) Timeline for notification to clients;
(c) Timeline for return of client's assets;
(d) Potential impact to other stakeholders.

The exit plan may also include the following in addition to the aforementioned components:

(a) Identification of potential impediments to the unwinding of the product or service, along with the corresponding measures remove or address impediments;
(b) Key responsible persons and workflow for implementation of exit plan;
(c) Protocol for cessation of test cases and return of data to clients and FSA;
(d) Risk management measures and client safeguard measures implemented during exit proceedings (e.g. safe processing and return / deletion of client data).

11.4.2 Exit Plan Submission

Following the initiation of discontinued service proceedings, the Case Officer will notify the applicant to submit a detailed exit plan to the Authority.

The applicant is required to submit the exit plan within 10 business days via the dedicated Sandbox mailbox.

If the applicant fails to submit the exit plan by the required deadline and is outstanding for 1 month, or if the applicant has failed to submit the exit plan with all the required components and the missing components are 1 month outstanding, the Authority reserves the right to undertake additional actions as prescribed under the FSA Act and the Securities Act and the Financial Service (Regulatory Exemption Sandbox) Regulations. This includes actions such as:

(a) Issuing a public censure;
(b) Imposing an administrative penalty; or
(c) Revocation of the exemption

Further details regarding the powers of the Authority are provided in the Regulations.

If the applicant has submitted the exit plan with all the required components, the exit plan will be moved to review.

11.4.3 Administrative Processes of Exit Plan

If the applicant has submitted the exit plan with all components required and within the agreed timeframe, the Authority will undertake internal review of the report. The process of the review for each component will be as follows:

Step 1: The Case Officer shall acknowledge receipt of the plan.

Step 2: The Authority shall carry out an internal review of the exit plan to assess whether the plan is adequate, viable, sound and effective in terminating the product / service with minimal impact to the applicant's clients.

Step 3: The Authority will provide feedback to the applicant (if any). The Case Officer will discuss and follow up on changes or additions to the exit plan with the applicant, and refine or revise the exit plan until it is deemed satisfactory to the Authority.

Step 4: The Applicant is responsible for providing a revised plan to the Authority for review, within the agreed upon timeframe.

Step 5: Determine if the (revised) exit plan is deemed to be adequate and sound. If the (revised) plan is deemed satisfactory by the Authority, the Case Officer will inform the applicant accordingly via the dedicated Sandbox mailbox, and notify the applicant that they may proceed with implementation of the exit plan. If the exit plan is not deemed satisfactory, the Case Officer will return the exit plan to the applicant for further discussion.

Following approval of the exit plan, the applicant should proceed with implementation of the exit plan and move towards cessation of its product or service.

The Authority will monitor and review the applicant's implementation of the proposed exit plan on an on-going basis, to ensure that the exit plan is executed in a timely and effective manner with minimal impediments or issues. If the Case Officer encounters any issues or concerns with regards to the applicant's exit, the Case Officer will notify the applicant of said concerns and discuss further to resolve any issues.

11.4.4 Third Party Confirmation

The applicant is required to provide independent third-party confirmation regarding the return of client assets and the cessation of their business, once the exit plan has been implemented and the business has been resolved. The applicant should seek external confirmation at the end of the proposed exit plan timeline. The external confirmation should be provided to the Case Officer via the dedicated Sandbox mailbox, letter, or via other formal methods of communication.

Upon receipt of the third party confirmation, the Case Officer will write to the applicant and acknowledge the confirmation, return of client assets, and the full cessation of the applicant's product or service.

If the applicant is unable to provide the required confirmations within the agreed upon timeframe, the applicant should request for delay in submission and provide valid explanations to the Case Officer. The Case Officer will review and determine if any delay in submission is allowed.

11.4.5 Closure Report for Discontinued Service

The applicant should have fully executed the exit plan, ceased and resolved all business, and provided of the third-party confirmation about the return of client assets and termination of the applicant's business in the Sandbox.

Following the execution of the exit plan in full (i.e. termination of product / service) and provision of third-party confirmation to the Authority, the applicant is to provide a closure report to the Case Officer within 5 business days of the end of the exit plan timeline.

The applicant's closure report should include, at a minimum, the following components:

(a) Confirmation from eligible persons of notification of exit to clients;

(b) Description and evidence of the resolution of the applicant's product or service, critical functions and assets;
(c) Description and evidence of the cessation of all business activities;
(d) Treatment of client assets, client data, and other findings (e.g. safe disposal of client data);
(e) Key timeline for the exit proceedings;
(f) Measures undertaken to discharge liabilities (if any);
(g) Description of outstanding issues (if any);
(h) Other measures undertaken to ensure minimal impact of discontinued service on clients;
(i) Potential disadvantages identified to any stakeholders in the discontinuation of service;
(j) Summary of Sandbox findings, issues or insights, along with feedback on the experience within the Sandbox.

If the applicant has failed to include the required components, the Authority will issue a reminder and the applicant should respond with the missing components within 3 business days.

If the applicant has provided all required components in the closure report and effectively ceased and resolved its business, the Case Officer will write to the applicant and acknowledge the closure report, inform the applicant that no further action is required, and that the applicant has successfully exited the Sandbox.

It should be noted that all relevant documents or information of an applicant, covering the entire Sandbox period shall be maintained by the Authority for record keeping purpose.

11.5 Transition to Formal Licensing / Deployment

11.5.1 Intended Transition to License

In the event that the applicant decides to transition to formal licensing and deployment, and is concurred by the Authority, the applicant will undergo review procedures to determine whether the applicant is able to obtain a formal license to launch its product / service in the market and begin the relevant license application procedures.

There are 2 outcomes for the applicant in the transition to formal licensing or deployment:

(a) The applicant undergoes the transition phase successfully and is moved to formal licensing and deployment by the Authorization team; or
(b) The applicant does not obtain approval for license application during transition phase, and will face discontinued service. In this case, the applicant will be required to cease its product or service and undertake the steps as described in the previous section.

11.5.2 Transition Plan Components

If the applicant intends to transition the applicant to formal licensing, with the approval obtained, a transition plan will be required. The objective of the transition plan is to ensure the applicant is able to receive formal licensing and deployment outside of the Sandbox environment in a smooth and timely manner.

The transition plan should include, at a minimum, the following components:

(a) Application for the appropriate license;
(b) Timeframe of notification to clients;
(c) Relevant materials to support license application (e.g. Sandbox performance summary);

(d) Proposed timeline and plan to launch the product or service outside of Sandbox;
(e) Controls, measures and safeguards to be implemented in event of deployment;
(f) Potential risks or impediments to formal licensing / deployment, and corresponding measures to be implemented to address and resolve issues;
(g) Changes to business, measures or parameters and reasons behind such changes (e.g. enhancement of controls implemented based on anticipated increase to client exposures);
(h) Procedures for return of client assets and other Sandbox information, where appropriate;
(i) Any other factors of consideration pertinent to the deployment of the applicant's product or service.

11.5.3 Transition Plan Submission

The transition plan is required to be submitted to the Case Officer within 10 business days upon the notification of the decision to the Case Officer via the dedicated Sandbox mailbox. The Case Officer will be responsible for reminding the applicant about the submission deadline.

If the applicant fails to submit the transition plan within the required timeframe and is 1 month outstanding, or if the applicant has failed to submit the transition plan with all required components with missing components 1 month outstanding, without valid reasons for the delay, the Authority will decide whether reject the applicant's request to transition to formal licensing. The Authority will inform the applicant accordingly via the dedicated Sandbox mailbox. The applicant will then be required to undertake procedures to resolve and discontinue its product / service, following the procedures outlined in Section 11.4 in these Guidelines.

If the applicant has submitted the transition plan with all the required components, the plan will be moved to review.

11.5.4 Administrative Processes of Transition Plan

If the applicant has submitted the transition plan with all components required and within the agreed upon timeframe, the Authority will undertake internal review of the plan. The process of the review for the plan will be as follows:

Step 1: The Case Officer shall acknowledge receipt of the plan via the Sandbox mailbox.

Step 2: The Authority shall carry out an internal review of the transition plan to assess the adequacy, viability, soundness, completeness and effectiveness of the transition plan.

Step 3: The Case Officer will provide feedback on the transition plan (if any) via the Sandbox mailbox. Feedback may include a request for further clarifications, or additional information, measures or controls to be considered in the transition plan.

Step 4: The Applicant is responsible for providing a revised transition plan to the Authority for review, within the agreed upon timeframe which will be determined by the Case Officer based on the complexity and level of effort required to revise the transition plan. The Authority will review the revised transition plan following re-submission.

Step 5: The Authority will determine if the (revised) transition plan is deemed to be satisfactory to the Authority. If the (revised) plan is deemed satisfactory, the Authority will approve on the transition plan. The Case Officer will notify the applicant of this decision and

acknowledge the transition plan, and the applicant can execute the transition plan and move towards formal licensing and deployment. If the (revised) plan is deemed unsatisfactory, the Authority will notify the applicant of this decision and that the applicant will be moved to product / service termination, and undergo exit proceedings as described in the previous section.

Following approval of the transition plan, the applicant should proceed with the execution of the transition plan and move towards formal licensing and deployment of its product / service.

The Authority will monitor and review the applicant's implementation of the proposed transition plan on an on-going basis, to ensure that the transition plan is executed in a timely and effective manner with minimal impediments or issues. If the Case Officer encounters any issues or concerns with regards to the applicant's exit, the Case Officer will notify the applicant of said concerns and discuss further to resolve any issues.

11.5.5 Third Party Confirmation

The applicant is required to provide independent third-party confirmation regarding the return of client assets in the exit of the Sandbox environment, once the transition plan has been implemented. The applicant should seek external confirmation once client assets and other Sandbox assets (e.g. data) have been returned and resolved. The external confirmation should be provided to the Case Officer via the Sandbox mailbox, letter, or via other formal methods of communication.

Upon receipt of the third party confirmation, the Case Officer will write to the applicant and acknowledge the confirmation.

If the applicant is unable to provide the required confirmations within the agreed upon timeframe, the applicant should request for delay in submission and provide valid explanations to the Case Officer. The Case Officer will review and determine if any delay in submission is allowed.

11.5.6 Closure Report for Discontinued Service

The applicant should have fully executed the transition plan, ceased all business within the Sandbox environment, and provided of the third-party confirmation about the return of client assets and termination of the applicant's business in the Sandbox.

Following the execution of the transition plan in full and provision of third-party confirmation to the Authority, the applicant must provide a closure report to the Case Officer within 5 business days of the end of the transition plan timeline, prior to submission of the licensing application and deployment outside of the Sandbox environment.

The applicant's closure report should include, at a minimum, the following components:

(a) Key timeline for the exit proceedings;
(b) Confirmation from eligible persons of notification of exit to clients,
(c) Treatment of client assets, client data, and other findings (e.g. safe disposal of client data);
(d) Measures undertaken to discharge risks or liabilities to stakeholders (if any);
(e) Description of outstanding issues (if any);
(f) Summary of Sandbox findings, issues or insights, along with feedback on the experience within the Sandbox; and

(g) An overview of the next step(s) they are undertaking with respect to the service or product.

If the applicant has failed to include all required components, the Authority will issue a reminder and the applicant should respond with respect to the missing components within 2 business days.

If the applicant has provided all required components in the closure report and effectively ceased and resolved its business within the Sandbox, the Case Officer will write to the applicant and acknowledge the closure report, inform the applicant that they have successfully exited the Sandbox.

It should be noted that all relevant documents or information of an applicant, covering the entire Sandbox period shall be maintained by the Authority for record keeping purposes.

12. Communication Protocol

Formal queries and communications (e.g. periodic reports) between the applicant and Case Officer will be conducted via the dedicated Sandbox mailbox. The applicant should typically respond to formal requests and queries within 1-2 business days, or at the earliest possible date.

Ad hoc queries or communications between the applicant and Case Officer may be conducted via the dedicated Sandbox mailbox, direct calls, or any means of communication established. The Authority reserves the right to utilise all methods of communication as they see fit in order to facilitate communications with the applicant.

In the event that there is a change in the Case Officer or designated Sandbox contact person for the applicant, the Authority will inform the applicant and provide contact details.

The applicant should provide ad hoc updates to the Case Officer for the purposes of on-going monitoring, on a weekly basis or at a frequency agreed upon with the Case Officer. The weekly updates could include the following components:

(a) Status update on the progress of testing or the applicant's testing performance;
(b) Issues encountered or anticipated throughout the course of experimentation;
(c) Insights or findings from the experimentation phase;
(d) On-going implementation of controls to facilitate risk management or client safeguard measures;
(e) Relevant news or industry updates that could impact the applicant's case.

The Authority will determine and inform the applicant of the protocol for ad hoc communication.

13. Role of the Authority

The Authority is conferred with powers of supervision over the Regulatory Sandbox and may in carrying out its supervisory functions over the Regulatory Sandbox:

(a) Issue directions;
(b) Request information or documents from applicants;
(c) Revoke an exemption;
(d) Impose further conditions on the applicant;

(e) Appoint a person to advise a Regulatory Sandbox applicant on the proper conduct of its business;
(f) Appoint a person to assume the control of the affairs of the applicant relating to the exempted business;
(g) Suspend an applicant granted under the Regulations for a period of time, or until the happening of an event, as the Authority considers appropriate.

The Regulations also impose duties on the Authority, most notably, the duty not to disclose any information to a third party except where authorized under the written law.

Appendix 1

Due Diligence Requirements

The completed **Questionnaire Form for Shareholders and Beneficial Owners** by all shareholders and ultimate beneficial owners who do not have a management position in the company should be accompanied by:

- 1 certified true copy of passport(s)
- 1 recent passport photograph, with an attestation at the back of the photo that the photo is a true likeness of the person and signed by an acceptable certifier
- 1 certified proof of residential address that is not older than three months e.g. utility bill (water and / or electricity) and / or bank statement and / or tenancy agreement
- 1 original bank reference from each bank with which you are affiliated and / or a report from Credit Rating Agency from Country of Residence (if available)
- a list of directorships, partnerships, other business interests or affiliations (if applicable)
- Police Character Reference / certificate (original) not older than three (3) months from the Country in which the applicant resides or its equivalent
- Tax Clearance Certificate from the Country in which the applicant resides or its equivalent
- Politically Exposed Person Self-Declaration Form
- Evidence of source of fund / wealth

The completed **Personal Questionnaire** Forms by all directors, securities dealer representative, compliance officer and key persons in connection with the application, should be accompanied by:

- 1 certified true copy of passport(s)
- 1 recent passport photograph, with an attestation at the back of the photo that the photo is a true likeness of the person and signed by an acceptable certifier
- 1 certified proof of residential address that is not older than three months e.g. utility bill (water and / or electricity) and / or bank statement and / or tenancy agreement
- 1 original bank reference from each bank with which you are affiliated and / or a report from Credit Rating Agency from Country of Residence (if available)
- Certified copies of stated higher academic qualifications
- Certified copies of stated professional qualifications
- Certified copies of stated membership to professional bodies
- Detailed job description of your proposed role or position
- Past Employment references (if applicable)
- Comprehensive and Up-to-date Curriculum Vitae
- A list of directorships, partnerships, other business interests or affiliations (if applicable)
- Police Character Reference / certificate (original) not older than three (3) months from the Country in which the applicant resides or its equivalent
- Tax Clearance Certificate from the Country in which the applicant resides or its equivalent
- Politically Exposed Person Self-Declaration Form

Due Diligence documents for entity shareholders should include the following:

(a) Companies

- Certificate of Incorporation
- Memorandum and Articles of Association
- Notice of situation of Registered Office or any change thereof
- Particulars of Directors and Secretaries
- Audited financial statements for the past 3 years
- Certificate of Good Standing

(b) Foundations

- Foundation Charter
- Register of Founder(s), Counsellor(s), Beneficiaries and Protector(s) (if applicable)
- Certificate of Good Standing

(c) Trusts

- Trust Deed
- Declaration of Trust
- Register of Trustee(s), Settlor, Beneficiaries and Protector(s) (if applicable)

(d) Limited Partnerships

- Limited Partnership agreement
- Register of General Partner(s) and Limited Partner(s)

Appendix 2

List of Constitutional Documents

Certified true copies of the following documents:

- Certificate of Incorporation
- Memorandum and Articles of Association
- Notice of situation of Registered Office or any change thereof
- Particulars of Directors and Secretaries
- Audited financial statements for the past 3 years