BOM/BSD 48/May 2024

BANK OF MAURITIUS

Guideline
for Regulatory Sandbox Authorisation

May 2024

TABLE OF CONTENTS

INTRODUCTION

The financial sector in Mauritius is undergoing an unprecedented digital transformation. Alongside this evolving environment, the development of Fintech is also gathering momentum. Recognising the benefits and opportunities of Fintech innovations for financial consumers, the Bank of Mauritius ("Bank") deems it important to promote Fintech initiatives in a regulatory environment in order to protect consumers, safeguard the integrity of the financial system and in the same vein contribute to the successful transformation of Mauritius into a smart International Financial Centre.

According to Section 11C of the Banking Act 2004, a financial institution, a licensee under the National Payment Systems Act 2018 or a body corporate may apply to the Bank for a Regulatory Sandbox Authorisation ('RSA') in such form and manner, and shall be accompanied by such documents, as the Bank may determine.

The RSA allows a sandbox entity to experiment with fintech, regtech or other innovation driven financial services falling under the supervisory purview of the Bank.

Purpose

The purpose of the Guideline for Regulatory Sandbox Authorisation ('Guideline') is to provide a framework for the issuance of RSAs by the Bank. This Guideline, while setting out the principles and objectives of the regulatory sandbox regime, provides an overview of the application process for an RSA as well as the information to be furnished by an applicant to the Bank and specifies the minimum ongoing obligations of sandbox entities.

Authority

This Guideline is issued under the authority of sections 11C and 100 of the Banking Act 2004, section 50 of the Bank of Mauritius Act 2004 and section 17 of the National Payment Systems Act 2018.

The Bank may in such circumstances as may be prescribed, exempt a person who has obtained regulatory sandbox authorisation from any regulatory requirement.

Scope of Application

This Guideline applies to a financial institution, licensee or body corporate (including a fintech company) which has been authorised by the Bank to participate in the Sandbox.

Effective date

This Guideline shall come into effect on 16 May 2024.

1. Interpretation

For the purpose of this Guideline –

"applicant" means a financial institution under the Banking Act, licensee under the National Payment Systems Act (NPSA) or other body corporate (including a fintech company) which intends to apply or has applied for an RSA to the Bank either on its own, in joint capacity or in collaboration with another body corporate;

"financial institution" has the same meaning as in the Banking Act;

"fintech" means technologically enabled financial innovations which could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services;

"fintech company" refers to a body corporate (including a start-up) that utilises or plans to utilise fintech but excludes a licensee or financial institution;

"licensee" has the same meaning as in the NPSA;

"regtech" or **"regulatory technology"** means the innovative technology solutions utilised by a financial institution and other regulated entities to facilitate compliance with regulatory requirements;

"Regulatory Sandbox" or **"Sandbox"** means a controlled testing environment which allows a financial institution, a licensee or a body corporate authorised by the Bank under Section 11C of the Banking Act to conduct experiments under the supervision of the Bank;

"regulatory sandbox authorisation" means an authorisation granted under Section 11C of the Banking Act which allows a financial institution, a licensee under the National Payment Systems Act or a body corporate to enter a regulatory sandbox to experiment with fintech, regtech or other innovation driven financial services falling under the purview of the central bank;

"sandbox entity" means a financial institution, a licensee or a body corporate (including a fintech company) which has been authorised by the Bank to participate in the Sandbox;

"user" refers to the natural person/entity availing of the product or service being offered by the Sandbox entity;

2. Eligibility criteria

2.1 An application for an RSA shall, as a minimum, comply with the following criteria:

a) Genuineness of innovation

The solution must be innovative enough to add value to the offer of financial services.

b) Genuine need for the RSA

The applicant must demonstrate:

i. a genuine need for support and testing of the solution on real users; and

ii. that the solution does not fit in the existing regulatory framework and/or can only be deployed with the exemption or relaxation of certain regulatory requirements, as may be sought.

c) Benefits to/protection of users

The solution should offer perceptible benefits to users and the financial system. The applicant should ensure adequate protection of users.

d) Risk management framework

The applicant should implement an appropriate risk management framework to ensure that the underlying risks are duly managed and mitigated such that there is no unnecessary risks to the soundness and stability of the financial system.

e) Readiness of the solution

The applicant should have conducted some prior testing and the solution should be sufficiently ready for deployment in the sandbox environment. The applicant must have adequate resources to conduct the testing. The testing plan should cover key outcomes, performance indicators and other measures of success during the testing period.

f) Broader scale deployment

The proposed exit and transition strategy shall demonstrate that the applicant has the capacity/resources and the intention to deploy the solution on a broader scale upon expiry of the RSA.

3. Potential risks and safeguards

3.1 An applicant shall identify the potential risks to users that may arise from the testing of the innovative financial services/solutions in the Sandbox and propose appropriate safeguards to address the identified risks.

3.2 The safeguards referred to in paragraph 3.1 may include, but are not limited to:

a) implementation of relevant policies and procedures on disclosures of the potential risks to users in the Sandbox and relevant confirmation from users that they fully understand and accept the risks;

b) restricting the number of users participating in the Sandbox and/or the number/value of transactions and ensuring that they understand and accept the risks to users;

c) restricting the users to a certain segment or profile;

d) limiting the duration of the testing period;

e) providing a user redress mechanism comprising financial compensation as deemed relevant;

f) deploying adequate and relevant resources for the testing; and

g) implementing relevant risk mitigation measures.

3.3 In assessing the risks and evaluating the proposed safeguards, the Bank shall give due regard to its regulatory objectives, including the following:

a) preserving sound financial and business practices consistent with financial stability;

b) promoting fair treatment of users;

c) preventing money laundering and countering of terrorism and proliferation financing;

d) protecting the confidentiality of user information; and

e) encouraging healthy competition in the banking and non-banking financial sectors.

4. Application and Authorisation process

4.1 An applicant shall ensure that the specified eligibility criteria are satisfied while submitting its application.

4.2 An applicant shall submit a duly completed application form, as available on the Bank's website at https://www.bom.mu/financial-stability/supervision/guidelines/guideline-regulatory-sandbox-authorisation, addressed to:

The Second Deputy Governor
Bank of Mauritius
Sir William Newton Street
PORT LOUIS

4.3 No application processing fee will be applied.

5. Determination of applications

5.1 The Bank shall assess the application based, *inter alia*, on the following parameters:

(i) profile of the applicant including the fitness and probity of the beneficial owners, shareholders, directors and senior officers;

(ii) compliance with eligibility criteria;

(iii) the potential benefits of the proposed innovative services;

(iv) the potential risks and mitigating measures/safeguards proposed to be applied;

(v) appropriateness of the applicant's internal risk management framework and control procedures including those related to Anti-Money Laundering and Counter-Terrorism Financing;

(vi) the integrity, capability and track record of the applicant; and

(vii) any other factors as may be determined by the Bank.

5.2 The Bank may also take into consideration the number of entities that can be effectively supported concurrently within the Sandbox at any time to ensure its smooth functioning.

Chart 1: Application and Authorisation process

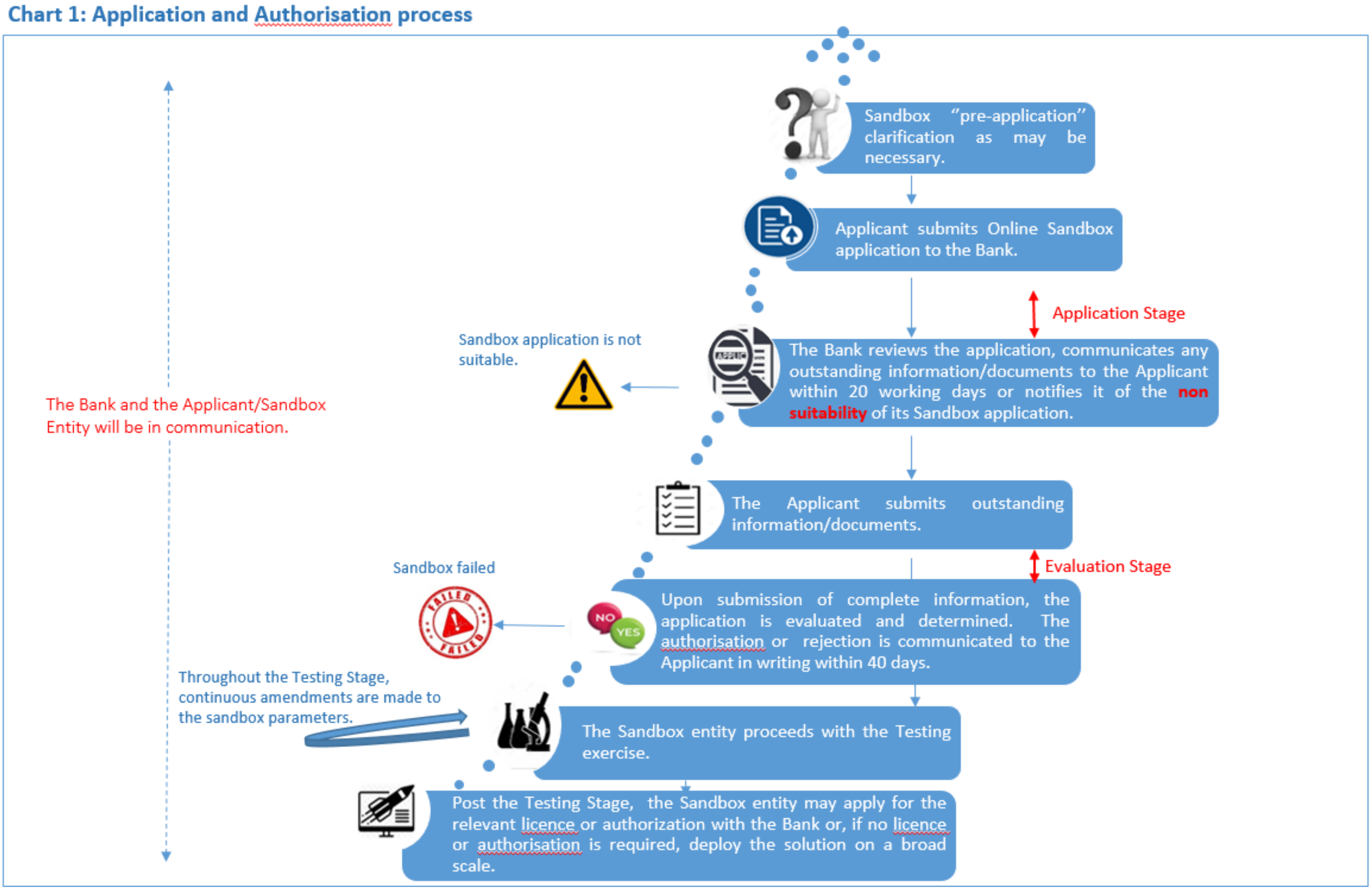
Chart 1: Application and Authorisation process
Application Stage
Evaluation Stage
Sandbox application is not suitable.
Sandbox failed
NO
YES

Sandbox "pre-application" clarification as may be necessary.

Applicant submits Online Sandbox application to the Bank.

The Bank reviews the application, communicates any outstanding information/documents to the Applicant within 20 working days or notifies it of the non suitability of its Sandbox application.

The Applicant submits outstanding information/documents.

Upon submission of complete information, the application is evaluated and determined. The authorisation or rejection is communicated to the Applicant in writing within 40 days.

The Sandbox entity proceeds with the Testing exercise.

Post the Testing Stage, the Sandbox entity may apply for the relevant licence or authorization with the Bank or, if no licence or authorisation is required, deploy the solution on a broad scale.

The Bank and the Applicant/Sandbox Entity will be in communication.

Throughout the Testing Stage, continuous amendments are made to the sandbox parameters.

5.3 The Bank shall within **20** working days from receipt thereof communicate to the applicant the outstanding information, request for clarification and/or information regarding the applicant's potential suitability for participation in the Sandbox or inform the applicant that the application cannot be entertained.

5.4 The Bank shall within 40 working days of receipt of a complete application, determine whether an authorisation can been granted or rejected.

5.5 The Bank shall inform the applicant of the outcome of its application.

5.6 In the event an authorisation is granted, the Bank shall issue a communique on its website to inform the public accordingly.

5.7 The Bank shall reject applications where –

a) the applicant fails to demonstrate compliance with the eligibility criteria;

b) the applicant fails to propose adequate mitigating controls and safeguards for identified risks;

c) it is not satisfied with the fitness and probity of the beneficial owners, shareholders, directors and senior officers as applicable; or

d) where there are concerns that the applicant shall be:

(i) undermining sound Know Your Customer (KYC) principles;

(ii) violating the privacy of users;

(iii) promoting the sale of fraudulent/illegal products or services;

(iv) engaging into mis-selling of products or services;

(v) in violation of the Financial Intelligence and Anti-Money Laundering Act, and any Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation guidelines or directives issued by the Bank;

(vi) creating risks to financial stability; or

(vii) in contravention of intellectual property or any other applicable laws.

5.8 The Bank shall work with the applicant to determine the specific regulatory requirements and conditions (including test parameters and control boundaries) to be applied to the proposed solution. The applicant shall then be required to assess if it is able to meet these requirements. If the applicant is able to meet the proposed regulatory requirements and conditions, the applicant shall be granted authorisation to test the proposed innovative solution(s) in the Sandbox.

6. Regulatory exemptions

6.1 Applicants shall make an application for the exemption/relaxation being sought from relevant provisions of the applicable regulatory framework.

6.2 The Bank shall consider exemptions/relaxations from certain regulatory requirements on a case-to-case basis, depending on the fintech solution to be tested.

6.3 The exemptions/relaxations from regulatory requirements will be applicable only during the testing period.

7. Testing Stage

7.1 The sandbox entity shall proceed towards the testing of its solution upon receipt of the RSA.

7.2 The sandbox testing shall be conducted for a maximum period of twelve (12) months. The testing period may, however, be extended, upon request of the sandbox entity for such period as may be determined by the Bank.

7.3 Each sandbox entity shall nominate a contact person to liaise with a designated officer of the Bank during the testing phase and for all other purposes.

8. Reporting requirements

8.1 The reporting requirements shall be communicated to the sandbox entity and shall as a minimum comprise of interim reports on the progress of the test during the testing period and a final report. All reports shall be signed by the Chief Executive Officer of the sandbox entity or a duly authorised officer.

<u>Interim reports</u>

8.2 The interim reports shall cover the progress of the testing as compared to the initial testing plan and include:

(i) updates on key performance indicators and milestones;

(ii) reasons of any observed delays not meeting the set milestones/key performance indicators;

(iii) a brief on incidents including fraud, cyber/IT related and other operational incidents covering the root cause, incurred/potential impacts and remedial measures;

(iv) the volume/number of transactions broken down by relevant categories of customer;

(v) details of complaints received; and

(vi) any other information required by the Bank.

<u>Final report</u>

8.3 The final report shall comprehensively cover the outcome of the testing (taking into considerations the items under (1) above) and the way forward. The report shall also cover lessons learned in case of failed testing.

9. Obligations of the sandbox entity towards the user

9.1 The following disclosures shall be made in clear terms by the sandbox entity:

a) the characteristics and any complexity of the product/service being proposed to users;

b) details on available compensation for losses incurred during the testing phase; and

c) that the Bank shall not be liable for any loss incurred by the users.

9.2 The users shall provide a written confirmation that they fully understand and accept the risks, disclosure and protection terms before signing up for any product or service being offered under the RSA.

10. Queries and Complaints

10.1 The sandbox entity shall implement appropriate and effective procedures for the handling of complaints. All complaints including details on their status/action taken shall be recorded in a complaint register.

10.2 Where a user is of view that his/her complaint has not been satisfactorily resolved by the sandbox entity, the user may refer the complaint to the Ombudsperson for Financial Services in the manner provided for in the Ombudsperson for Financial Services Act.

10.3 Users may also address general queries to the Bank *via* e-mail to regulatorysandbox@bom.mu.

11. Confidentiality and Data Protection

11.1 A sandbox entity shall implement relevant measures for protecting the confidentiality of information of its users, during the testing period and after its exit from the Sandbox. The sandbox entity shall ensure that all its employees or any other persons appointed by it who receive confidential information of users in the course of their duties shall be subject to the confidentiality obligations, including after the termination of their duties.

11.2 A sandbox entity shall ensure compliance with the Mauritian Data Protection Act 2017 and other applicable data protection laws.

12. Request for renewal of RSA or exit from the Sandbox

12.1 The sandbox entity shall, at least 45 days prior to the expiry of the testing period, either:

(a) inform the Bank of its intention to exit the Sandbox at the end of the testing period and provide its exit plan and the report as specified at paragraph 8.3; or

(b) apply to the Bank for the renewal of its RSA and submit the rationale thereof as well as the report as specified at paragraph 8.3.

12.2 Where the Bank is satisfied with the request of the sandbox entity under paragraph 12.1 (b) above, it may renew the RSA for such specified period and on such conditions as it may determine.

12.3 The authorisation granted to the sandbox entity as well as any regulatory requirements exempted or relaxed by the Bank shall expire at the end of the testing or renewal period. The sandbox entity shall be required to ensure that the exit process is duly completed within 20 days prior to the expiry of the testing period.

12.4 Upon exit and where the Bank is satisfied with the successful completion of the testing, the sandbox entity shall have the following options, as applicable:

(i) apply for any relevant licence or authorisation from the Bank or

(ii) where no new licence or authorisation is required, deploy the solution on a wider scale.

12.5 Notwithstanding the above, the sandbox entity may, subject to the written approval of the Bank, exit the Sandbox during the testing period, by giving prior written notice of at least 20 working days to the Bank of its intention to exit the Sandbox, as well as the effective date of the exit. Where the Bank grants its written approval for exit from the Sandbox, the sandbox entity shall ensure that the exit process is completed by the effective exit date communicated to the Bank and the report specified at paragraph 8.3 is duly submitted to the Bank. The sandbox entity shall thereafter surrender the RSA to the Bank.

12.6 No approval for exit shall be granted by the Bank to a sandbox entity unless it is satisfied that the interests of users are safeguarded, and that all conditions of its exit have been complied with.

12.7 The sandbox entity shall inform its users that it is exiting the Sandbox as soon as it receives an exit approval from the Bank.

12.8 The Bank shall issue a communiqué on its website when it grants an approval for a sandbox entity to exit the Sandbox.

12.9 The sandbox entity shall ensure that any existing obligation towards the users are completely fulfilled or addressed before exiting the Sandbox or before discontinuing the sandbox testing.

12.10 The sandbox entity shall maintain, for a period of at least 7 years, records of acknowledgement from all its users that all its obligations towards them have been met prior to the exit.

13. Records

13.1 Every sandbox entity shall keep, in relation to its activities, a full and true written record of every transaction it conducts under the Sandbox. Such records shall include:

(i) accounting records;

(ii) all transactions conducted with its users;

(iii) acknowledgement from all its users that all its obligations towards them have been met; and

(iv) such other records as the Bank may determine.

13.2 Every record under paragraph 13.1 shall be kept:

(i) in written form or kept on microfilm, magnetic tape, optical disk, or any other form of mechanical or electronic data storage and retrieval mechanism as the Bank may agree to;

(ii) for a period of at least 7 years after the completion of the transaction it related to; and

(iii) in such place as may be approved by the Bank.

14. Variation of conditions, Suspension or Revocation of sandbox authorisation

14.1 The Bank may amend, vary or cancel any of the conditions under which the RSA has been granted, or impose new conditions as permissible under the Banking Act.

14.2 Without prejudice to the powers of the Bank to revoke an RSA, where the sandbox entity fails to comply with the provisions of applicable legislation or any condition attached to the RSA, the Bank may suspend the RSA for such period and subject to such terms and conditions, as may be specified.

14.3 The Bank shall not suspend an RSA under paragraph 14.2 unless the sandbox entity is given:

(a) prior written notice of the intention of the Bank to suspend the RSA and the reasons for doing so not less than 14 days; and

(b) an opportunity to make representations on the matter.

14.4 Notwithstanding anything contained in paragraphs 14.2 and 14.7, where the Bank is satisfied on reasonable grounds that it is urgent and necessary to do so in the interests of the sandbox entity's users, the financial system or the general public, it may suspend the RSA immediately without prior notice, and provide an opportunity to the sandbox entity to make representations, within 7 days of the effective date of suspension. If the response is satisfactory, the Bank may reinstate the RSA. In any other case, the Bank shall, within 14 days of the representations made and after considering those representations, notify the sandbox entity of its final decision.

14.5 The Bank may revoke an RSA at any time before the end of the testing period, if the sandbox entity:

a) fails to carry out the safeguards referred to in paragraph 3.2;
b) submits false, misleading or inaccurate information, or has concealed or failed to disclose material facts in the application;
c) contravenes any applicable law administered by the Bank or any applicable laws in Mauritius or abroad which may affect the sandbox entity's integrity and the reputation of Mauritius;
d) goes into receivership or liquidation, is wound up or otherwise dissolved;
e) breaches data security and confidentiality requirements;
f) carries on business in a manner detrimental to users or the general public;
g) fails to effectively address any technical defects, flaws or vulnerabilities in the product, service or solution which gives rise to recurring service disruptions or fraud incidents;

h) fails to implement any guidelines, instructions or directives issued by the Bank;

i) fails to comply with the terms and conditions of its suspension under paragraphs 14.2 and 14.4 within the specified timeframe; and/or

j) its shareholders, senior officers and directors are no longer considered as fit and proper by the Bank.

14.6 In addition to the revocation of the RSA, appropriate actions under the relevant regulatory frameworks in Mauritius may be initiated against the sandbox entity and/or its officers.

14.7 When revoking the RSA, the Bank shall:

a) require the sandbox entity to immediately suspend trials on new users i.e. no new users should be permitted to sign up for using/testing the solution;

b) give the sandbox entity 30 days’ prior notice of its intention to revoke the authorisation unless provided otherwise in the Banking Act; and

c) provide an opportunity to the sandbox entity to make representations to the Bank on the revocation and the grounds thereof.

14.8 Upon revocation of an RSA, the sandbox entity shall be required to:

a) immediately implement its exit plan to cease its activities;

b) notify its users about the cessation and their rights to grievance and/or redress, as applicable;

c) submit a report to the Bank on the actions taken, within 10 days of the revocation or within such period as may be specified by the Bank; and

d) comply with any other instructions, guidelines or directives issued by the Bank.

Bank of Mauritius
16 May 2024