

**OUTSOURCING
GUIDELINES**
**For Banks and Other Financial
Institutions**
December 2021

Central Bank of Seychelles
Financial Surveillance Division

OUTSOURCING GUIDELINES

Central Bank of Seychelles

Table of Contents

1. INTRODUCTION.....	3
2. APPLICABILITY.....	3
3. GLOSSARY.....	3
4. ROLE OF THE BOARD OF DIRECTORS AND MANAGEMENT.....	4
5. OUTSOURCING POLICY.....	5
6. AGREEMENT	5
7. RISK ASSESSMENT	6
8. DUE DILIGENCE	6
9. BUISNESS CONTINUITY PLAN	7
10. DATA CONFIDENTIALITY AND SECURITY.....	7
11. ROLE OF THE SUPERVISORY AUTHORITY	8
11. LIST OF INFORMATION TO BE SUBMITTED	8

OUTSOURCING GUIDELINES

Central Bank of Seychelles

1. INTRODUCTION

Financial Institutions are increasingly using third party services to carry out activities, functions and processes as outsourcing arrangements to meet new and complex challenges such as innovation in technology, increasing competition, economies of scale and improvement in quality of service to stakeholders.

Outsourcing¹ activities are classified into two categories, these are namely material and non-material activities.

2. APPLICABILITY

These guidelines are applicable on all future outsourcing arrangements and those previously entered into by financial institution and other entities² (hereafter also referred to as the institutions) in Seychelles regulated by the Central Bank of Seychelles. All new outsourcing arrangements shall be governed under this guideline and outsourcing provisions set out in section 11 of the National Payment System Act, 2014 (NPSA) as applicable. Henceforth, in accordance with relevant provision in the amendments of the Financial Institutions Act, 2004, as amended and that of the NPSA related to outsourcing, financial institutions are required to seek authorisation from the Central Bank of Seychelles prior to entering into an outsourcing arrangement.

3. GLOSSARY

- 3.1 Board of Directors** - The highest body of authority in an institution responsible for the strategic guidance of the financial institution, the effective monitoring of its management, and accountability to its shareholders.
- 3.2 Central Bank**³ - The Central Bank of Seychelles established by the Central Bank of Seychelles Act 2004.
- 3.3 FIA** – The Financial Institutions Act, 2004, as amended.
- 3.4 Financial Institutions** – Any bank or bureau de change⁴ or any other institution as may be determined by the Central Bank of Seychelles.
- 3.5 Management** – Persons having authority and responsibilities for planning directing and controlling the activities of the entity, directly or indirectly, including any directors (whether executive or otherwise of the entity).

¹ Defined as a regulated entity's use of a third party (affiliated entity or un-affiliated) to perform activities, functions or processes normally to save money, time and/or use the skills/technology of another entity on a continuing basis that would normally be undertaken by financial institutions, now or in the future.

² Development Bank of Seychelles, Housing Finance Company Limited and Seychelles Credit Union.

³ Section 2 of the FIA.

⁴ Section 2 of the FIA.

- 3.6 Material** - An outsourcing activity of such importance that any weakness or failure in the provision of this activity could have a significant impact on the institution's ability to meet its regulatory responsibilities or to continue its business.
- 3.7 Non-material** – Outsourcing activities that do not affect the internal control system to a large extent and consequently does not pose a significant risk. Moreover, non-material activities are generally statutory or cannot legally be provided by institutions, such as statutory audits, any discreet advisory services, including legal opinions. These activities are also considered very low-risk, for instance, courier, mailing and printing services.
- 3.8 NPSA** – National Payment System Act, 2014.
- 3.9 NPSR** – National Payment System (Licensing and Authorisation) Regulations, 2014.
- 3.10 Payment Services** - services listed in the Schedule of the NPSA.
- 3.11 Payment Service Provider** – Any entity providing payment services.
- 3.12 Provider** – A person or organization providing the outsourced activity⁵.
- 3.13 Regulatory body** – A public or government entity that is set to exercise regulatory function. This involves imposing requirements, conditions or restrictions, setting standard for activities, enforcing regulation and obtaining compliance.
- 3.14 Stakeholder** – A party that has an interest in a company. The primary stakeholders in a company are generally investors, employees, customers and suppliers.

4. ROLE OF THE BOARD OF DIRECTORS AND MANAGEMENT

- 4.1** The Board of Directors and Management of financial institutions have the responsibility for ensuring that an effective risk management system on outsourcing is in place. The Board of Directors shall, at a minimum be responsible for:
- i. Approving the policy on outsourcing.
 - ii. Assessing how the outsourcing arrangement will support the institutions' objectives and strategic plan.
 - iii. Approving material outsourcing activity.
 - iv. Assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures as commensurate with the nature, scope and complexity of the outsourcing arrangements.
- 4.2** Management has the responsibility for proper management of risks associated with outsourcing activities, and is responsible for:
- i. Evaluating the risk and materiality of the outsourcing activity.

⁵ Section 2 of the NPSA.

- ii. Implementing sound and prudent outsourcing policies and procedures approved by the Board.
- iii. Monitoring and controlling all relevant aspects of outsourcing arrangements on an ongoing basis.
- iv. Keeping the Board informed on material outsourcing risks in a timely manner.
- v. Ensuring that contingency plans, including availability of alternative service providers, costs and resources required to switch service providers are in place.
- vi. Ensuring that the internal audit function and the external auditors have the authority to assess any outsourced functions.
- vii. Ensuring that regulatory requirements on outsourced activities are complied with at all times.

5. OUTSOURCING POLICY

5.1 The institutions should have a policy approved by its Board of Directors on its approach to outsourcing. The Board of Directors retains responsibility for the outsourcing policy and the activities undertaken.

- i. The policy shall include at a minimum, the roles and responsibilities of all stakeholders, materiality assessment criteria, vendor management⁶, risk assessment and mitigation for risks associated with outsourcing, contingency plan and exit strategy from the outsourcing arrangement.
- ii. The institutions must recognise that no form of outsourcing is risk free. The policy should recognise the management of both material and non-material outsourcing of activities, such that it is proportionate to the risk it presents.
- iii. The policy should explicitly consider the potential effects of outsourcing certain significant functions (e.g. internal audit function) when conducting the risk analysis prior to outsourcing.
- iv. The institutions should specify the responsible unit or individual(s) responsible for monitoring and managing the outsourcing arrangement. Essentially, the financial institution must ensure that the responsible staff are trained to have reasonable understanding on the outsourcing and the outsourced activities.

6. AGREEMENT

6.1 All outsourcing arrangements should be subject to a comprehensive and legally binding agreement.

- i. The outsourcing activity should be clearly defined in the agreement.
- ii. The scope of the outsourcing activity should be clearly defined in the agreement along with the timeframe for implementation.
- iii. The respective rights and obligations of the institutions and the outsourcing service provider should be precisely defined and specified. This should also serve to ensure compliance with laws and applicable supervisory regulations and guidelines for the duration of the outsourcing arrangement.
- iv. The agreement should include a termination and exit management clause, in the event of default or failure by the service provider.

⁶ i.e. due diligence, on-boarding, contractual requirements, monitoring, training and development.

- v. The agreement should have a provision in regards to contingency planning.
- vi. The contract should cover the protection of confidential information, banking secrecy and any other specific provisions relating to handling confidential information. Whenever information is subject to confidentiality rules at the level of the institutions at least the same level of confidentiality should be ensured by the service provider.
- vii. The agreement must contain a penalty clause in the event that the service provider fails to provide services as mutually agreed.
- viii. In entering into the agreement, the institutions shall ensure that no outsourcing arrangement is made with the service provider having close relationship with the management or employees of the institutions, which may create a conflict of interest.
- ix. The agreement should ensure that the service provider's performance is continuously monitored and assessed so that any necessary corrective measures can be taken promptly.
- x. The agreement should not consist of clauses that would hinder the Central Bank from exercising its supervisory powers. Additionally, the Central Bank should have the same right of access to information with the service provider as it has with the institutions having undertaken the outsourcing.

7. RISK ASSESSMENT

- 7.1 The institutions must ensure that the proposed outsourcing activity has been subject to a comprehensive risk assessment, and that all the risks identified have been adequately addressed prior to initiating the outsourced activity.
- i. The risk assessment shall cover the importance and criticality of the services to be outsourced.
 - ii. The rationale for the outsourcing.
 - iii. The impact that the outsourcing activity may have on the institutions' risk profile.
 - iv. The risk assessment should include assessment of the specific arrangements underlying the services being offered, the service provider, and the location from which the services are to be provided.
 - v. The risk assessment should also include the risk mitigation strategies in place to address identified risks.
 - vi. The institutions must re-perform the risk assessment after implementing the outsourcing activity. The re-assessment must be in line with the institutions' risk management framework.
 - vii. In addition to the risk assessment, a comprehensive due diligence on the nature, scope and the service provider needs to be performed to identify and mitigate key risks.
 - viii. The risk assessment must cater in addressing arising risks resulting from a temporary disruption to service, to that of a breach in security and confidentiality, and unexpected termination in the outsourcing arrangement.

8. DUE DILIGENCE

- 8.1 Prior to selecting a service provider and entering into an agreement, the institutions should perform stringent due diligence on the service provider. The institutions should develop criteria that would enable them to select service providers that have the ability and capacity and ability, both operationally and financially, to perform the outsourced activities.
- i. The information to be evaluated must be based on the service provider's financial soundness, experience, reputation, performance standards and technical capabilities.

- ii. The due diligence shall also address other issues, such as potential conflicts of interest in case service provider is a related/affiliated party, or where it provides similar services to competitors. The institutions shall also identify all potential and actual conflicts in order that such are avoided or discreetly managed.
- iii. The due diligence and selection process shall take into account the service provider's ability to meet obligations as per the requirements of the institutions.
- iv. The analysis of the due diligence performed shall be documented and re-performed (depending on the timeframe the services is to be offered), as part of the monitoring and control processes of the outsourcing arrangement.

9. BUSINESS CONTINUITY PLAN

9.1 The institutions must have a business continuity plan in place based on realistic and probable disruptive scenario. Subsequently, financial institutions must establish and maintain a plan for disaster recovery and periodic testing of the contingency plan.

- i. The institutions should take appropriate steps to assess and address the potential consequence of a business disruption.
- ii. The business continuity plan should enable the institutions to continue business operation in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement.
- iii. The business continuity plan should address the issues such as availability of alternative service providers and hand-over process to a new acceptable supplier.
- iv. For assurance on the functionality and effectiveness of its business continuity plan, the institutions must carry out regular testing and review of the plan.

10. DATA CONFIDENTIALITY AND SECURITY

10.1 The institutions that engage in outsourcing should take appropriate steps to protect confidential information.

- i. The institutions should prohibit service providers from disclosing customer information to any third-party except for regulatory purpose.
- ii. In reference to section 6.1(vi), the outsourcing agreement should contain a clause that addresses the service provider's responsibility for confidentiality and security.
- iii. The institutions, before providing data to third party, shall ensure that proposed outsourcing arrangement complies with the relevant statutory/regulatory requirements related to confidentiality of its customers.
- iv. Depending on the nature of the outsourcing arrangement, the institutions should consider the possibility of notifying their customers in advance that customer data may be transmitted to a service provider as part of their contractual arrangement with the customers.
- v. In cases where outsourcing arrangements involve disclosure of confidential customer information to service provider, the institutions shall seek consent of the customer and notify the Central Bank accordingly.
- vi. The institutions must ensure that outsourcing activity does not violate any statutory/regulatory requirements on Anti-Money Laundering as per the Anti-Money Laundering and Countering the Financing of Terrorism Act, 2020.

11. ROLE OF THE SUPERVISORY AUTHORITY

11.1 The responsibility of the Central Bank as the regulatory body, should ensure that any outsourcing arrangements do not hamper the ability of the regulated institutions to meet its regulatory requirements.

- i. The regulator should aim to be satisfied that institutions ensure that their outsourcing agreement with service providers grant the regulatory body the right to information and the right to give directions or instructions, where necessary, which the regulatory body needs to exercise its supervisory functions.
- ii. The regulator must ensure that the outsourced activity is not an ownership or management function, as the onus should fall on the institutions' management itself and should not be outsourced.
- iii. The regulatory body should aim to ensure that their powers to issue orders or instructions to the outsourcing institutions can be reliably enforced, without being compromised by instructions issued to the service provider by other bodies, so as to ensure the orderly performance of the outsourced activities.
- iv. The regulator must determine that the institutions have established appropriate policies and processes to assess, manage and monitor outsourced activities.

12. LIST OF INFORMATION TO BE SUBMITTED

12.1 In seeking the approval of the Central Bank for an outsourced activity and in order to process the request, the institutions are required to submit the following documents:

- i. Outsourcing policy approved by the Board.
- ii. A statement on the rationale for outsourcing.
- iii. Profile of the service provider.
- iv. A draft outsourcing agreement to be entered between the institution and the service provider.
- v. Contingency plan of the outsourcing arrangement.
- vi. A written document whereby Board of Directors has given its approval for the outsourcing arrangement.
- vii. Risk assessment performed on the outsourced activity
- viii. Assurance that all the internal control procedures and risk management systems are in place for the implementation of the outsourcing.
- ix. Any other relevant information as may be required by the Central Bank.

Along with information listed above, in outsourcing an individual, the financial institution is required to submit the following documents:

- i. Detailed curriculum vitae
- ii. Two character references
- iii. Independency of the individual from the financial institution
- iv. Disqualification of the individual
- v. Police character certificate
- vi. Declaration of being/not being a Politically Exposed Person

- vii. Legal notarised proof of residential address less than 3 months' old
- viii. Certified copy of passport
- ix. Banker's reference to which the individual has maintained its account over a 10-year period with the bank.
- x. Personal information form (Annex 1)

12.2 Moreover, in regards to payment services, along with information listed in section 12.1, the following information needs to be submitted in accordance to schedule IV of the NPSR,;

- 1) The identity of persons responsible for the management of the specific payment service activities.
- 2) A signed document detailing the features and operational modalities of all IT systems used/proposed to be used, including the operating systems, software and interfaces explaining at a minimum the following-
 - (a) a description (including diagrams) of the configuration of the applicant's payments technological platform and its capabilities showing-
 - (i) how such system is linked to other host systems or the network infrastructure of the applicant;
 - (ii) how transaction and data flow through the network, settlement process and timing;
 - (iii) the types of telecommunication channels and remote access capabilities that exist (e.g. direct modem dial-in, internet access, or both); and
 - (iv) the security controls/measures installed;
 - (b) a list of software and hardware components indicating the purpose of the software and hardware in the infrastructure;
 - (c) how data security and data integrity is ensured;
 - (d) how the platform interacts at the technical level with other payment systems.
- 3) Internal control and audit mechanisms which the applicant proposes to establish in order to comply with the Anti-Money Laundering Act, and Countering the Financing of Terrorism Act, 2020 and the Prevention of Terrorism Act, 2021, as amended.
- 4) Details of the customer protection measures, including complaints handling mechanisms and consumer awareness program relating to the payment service.
- 5) Details of data protection policy.

Annex 1: Personal Information Form

Surname	
First Name	
Second name	
Maiden name	
Any change in name apart from maiden name	
Gender	
Marital status	
Date of birth	
Place of birth	
NIN (where Seychellois)	
Present address	
Contact number	
Nationality	
Passport number	
Present occupation and place of occupation	
Businesses owned / part-owned	
Business address	
Spouse/partner name	
Mother's name	
Father's name	