

# OUTSOURCING GUIDELINE

FOR FINANCIAL INSTITUTIONS



# Contents

A. OVERVIEW .....	3
Introduction .....	3
Authority .....	4
Scope of application .....	4
Effective Date .....	4
Definitions .....	4
B. CLASSIFICATION OF OUTSOURCING ACTIVITIES .....	7
Outsourcing of Material Activities .....	7
Activities not considered to be outsourcing .....	8
Activities that cannot be Outsourced .....	9
Outsourcing Outside The Gambia ("Offshoring") .....	9
Intra-Group .....	10
Cloud-based Services .....	11
C. MANAGEMENT OF OUTSOURCING RISK .....	13
Outsourcing Management Plan .....	13
Business-Continuity Plan .....	15
Risk Management Framework in Outsourcing .....	16
Policy Formulation .....	16
Role of the Board of Directors and Senior Management .....	17
Evaluation of Risks Involved in Outsourcing .....	18
Due Diligence in Selecting Service Providers .....	18
Contract Issues & Service Level Agreement .....	19
Contingency Planning .....	21
Confidentiality and Security .....	22
Role of the External Auditor .....	22
Application of the Guideline .....	22
Annual reporting .....	23
D. REGULATORY PROCESS .....	23
Approval for outsourcing arrangements .....	23
Sanctions for Non-compliance .....	25

## A. OVERVIEW

### Introduction

1. Outsourcing refers to recourse to third-party service providers ("service providers") by financial institutions to perform activities on a continuing basis. With the evolution of technology, an increasing range of outsourcing of financial services activity is likely to be undertaken. Financial institutions usually outsource part of their activities with the view to reducing costs, which in turn may promote efficiency. However, outsourcing exposes financial institutions to new and/or increased risks. It may also impede effective supervision by regulators and have destabilising effects on the financial system. These risks should be controlled by requiring financial institutions to adopt a sound risk management framework when having recourse to outsourcing.
2. An essential criterion of Principle 25 (Operational risk) of the *Core Principles for Effective Banking Supervision* issued by the Basel Committee on Banking Supervision calls upon supervisors to determine that financial institutions have established appropriate policies and processes to assess, manage, and monitor outsourced activities.
3. This Guideline is prepared in-line with the guiding principles on outsourcing by Basel/Joint Forum guideline on Outsourcing in Financial Services 2005.
4. This Guideline on Outsourcing by financial institutions ("Guideline") is being issued to address risks associated with outsourcing in the Financial system through the application of an appropriate regulatory framework in this respect.
5. The main objective of this Guideline is to set out a broad framework for financial institutions that have entered outsourcing or are planning to outsource their business activities to service providers. The Guideline does not cover comprehensively all the outsourcing related issues but is intended to assist

financial institutions to identify the nature of risks involved and to address them effectively in view of the consideration that the Central Bank of The Gambia ("Bank") will hold its licensees fully responsible for all outsourced activities. The Guideline is based on a three-tier classification of activities, namely:

- material activities which require the authorisation of the Bank;
- non-material activities which also require authorisation; and
- core activities which cannot be outsourced.

#### Authority

6. This Guideline is issued under the authority of the Central Bank Act 2018, Section 71.3 and the Banking Act 2009.

#### Scope of application

7. This Guideline applies to all financial institutions licensed by the Bank under the Banking Act 2009 and should be read in conjunction with the Banking Act 2009, Non-bank financial institutions Act 2016, and Central Bank Act 2018 (and any successor acts thereof), as well as issued directives, notices and other guidelines issued by the Bank.

#### Effective Date

8. This guideline shall come into effect as from **January 31, 2023**.

#### Definitions

9. For the purposes of this policy document-

**"Bank"** means the Central Bank of The Gambia;

**"Outsourcing"** means an arrangement whereby a Financial Institution engages a third-party service provider to perform activities on an ongoing basis that would normally have been undertaken by the financial Institution itself;

**"Material outsourcing"** means the outsourcing of an activity of such importance that any weakness or failure in the provision of this activity could have a significant impact on the financial Institution's ability to meet its regulatory responsibilities and/or to continue in business;

**“Offshoring”** in the context of outsourcing means outsourcing activities beyond national borders;

**“Third-party service provider”** refers to an entity that is undertaking the outsourced activity on behalf of the Financial Institution and includes a member of the corporate group to which the Financial Institution belongs or an entity that is external to the corporate group, whether located in The Gambia or abroad;

**“Activity”** refers to a business or operational function, process or system;

**“Related Party”** refers to the financial institution, its Affiliates, directors, employees, external auditors, solicitors, and agents.

**“Affiliate”**, in relation to an entity, refers to any entity that controls, is controlled by, or is under common control with, the outsourcing entity.

**“Board”** means the board of directors of a financial institution, including a committee of the board where responsibilities of the board as set out in this policy document have been delegated to such a committee;

**“Customer”** refers to any person who uses, has used or may be intending to use, any financial service or product including—

- (i) a representative of the customer (such as the parents of a minor and authorised representative); and
- (ii) a person who has entered or intends to enter into arrangements with a financial institution (such as a guarantor or third-party security provider) on account of or for the benefit of a customer;

**“Customer information”** refers to any information relating to the affairs or the account, of any customer of a financial institution in whatever form including in the form of a record, book, register, correspondence, other document or material;

**“Material outsourcing arrangement”** refers to an outsourcing arrangement which—

(i) in the event of a service failure or security breach, has the potential to significantly impact the financial institution's provision of financial services to customers, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements; or

(ii) involves customer information and in the event of unauthorised access, disclosure or modification, or loss or theft of the information, has a material impact on the customer or Financial Institution;

(iii) In assessing whether an outsourcing arrangement is material and avoidance of doubt, any arrangement involving internal control functions (i.e. risk management, internal audit and compliance) would generally be considered as a material outsourcing arrangement;

**“Outsourcing arrangement”** refers to an arrangement in which a service provider performs an activity on behalf of a financial Institution on a continuing basis, where the activity would otherwise be undertaken by the Financial Institution;

**“Outsourcing risk”** refers to risk emanating from outsourcing arrangements that could result in a disruption to business operations, financial loss or reputational damage to a Financial institution.

**“Senior management”** refers to the Chief Executive Officer and senior officers of a Financial institution;

**“Service provider”** refers to an entity, including an affiliate, providing services to a Financial Institution under an outsourcing arrangement;

**“Sub-contractor”** refers to any entity, including an affiliate, which performs the whole or a part of the outsourced activity for the primary service provider;

**“Secondary service provider”** An entity which a service provider contracts for the provision of outsourcing services;

**“Cloud-based services”** or **“Cloud”** refer to the set of on-demand computing resources provided over the internet on a pay-per use basis;

**“Financial institution”** means any bank, non-bank deposit taking institution or cash dealer licensed by the Central Bank of The Gambia;

## B. CLASSIFICATION OF OUTSOURCING ACTIVITIES

### Outsourcing of Material Activities

8. Material outsourcing refers to the outsourcing of an activity of such importance that any weakness or failure in the provision of this activity could have a significant impact on the financial Institution’s ability to meet its regulatory responsibilities and/or to continue in business. Outsourcing of activities may have varying degrees of materiality in different Financial Institution. It is the role of management to evaluate whether an outsourcing arrangement is material or not. In assessing materiality, both quantitative and qualitative judgments are involved. A Financial Institution may carry out, as a minimum, the following assessment to determine the degree of materiality of an outsourcing activity:

- I. the relative importance of the business activity to be outsourced which can be measured in terms of contribution to income and profit;
- II. the potential impact of the outsourcing activity on current and projected earnings, solvency, liquidity, funding, capital, and risk profile;
- III. the impact on the Financial Institution’s reputation in case the service provider fails;
- IV. the cost of the outsourcing as a percentage of total operating costs; and
- V. the ability to maintain appropriate internal controls and meet regulatory requirements in the event of operational failures by the service provider.
- VI. The aggregate exposure to a particular service provider, in situations where the financial institution outsources various functions such as customer service officers, transaction officers, messengers, Drivers and any other operation services to the same service provider.

Note: The total number of outsourced staff of any department within the financial institution must not exceed 25% of the total number of staff in that department. E.g., where there are ten (10) staff in a department, the total outsourced staff cannot be more than 2 or 3.

Also note that approval to outsourced is limited to Persons/Service providers who are not directly or indirectly involved in banking services.

9. Financial institutions that intend to outsource certain managerial and internal control functions including compliance and internal audit should refer to Section 13. Furthermore, it should be recalled that an outsourcing contract, which was previously not material may subsequently become material resulting from an increase in volume or nature of the activity outsourced to the service provider or for any other reason.

10. A financial institution that intends to outsource any activity is required to notify and obtain the prior authorization of the Bank. Such authorization should be sought at least 15 working days before entering into an agreement with the service provider. The Bank may require additional information from the outsourcing financial institution and service providers depending on the specificities of the outsourcing arrangements.

Activities not considered to be outsourcing

11. There are certain types of activities which are not considered to be outsourcing as they do not affect or have an impact on the internal control activities of a financial institution. Such activities include:

- I. Common network infrastructures such as Visa and MasterCard.
- II. Financial information services such as Bloomberg etc;
- III. Services such as statutory audits, advisory services including legal opinions; and
- IV. Those activities which are generally considered very low-risk, for instance, courier, mailing, and printing services.



12. Financial institutions should ensure that adequate risk management procedures are always in place. The Board of Directors and Management should be fully aware of and responsible for the outsourcing of non-material activities.

#### Activities that cannot be Outsourced

13. A financial institution would not be allowed to outsource certain core activities. These activities should remain within the organisation in order to not lose control. Certain activities, if outsourced, might affect Management's ability to run the business properly. Activities that are considered 'core' and should not be outsourced are;

- I. Board and senior management functions such as strategic oversight, investment in portfolio decisions;
- II. Internal audit function;
- III. Compliance functions with Anti-Money Laundering and Combating of Financing and Terrorism and Know Your Customer (KYC) norms for opening accounts;
- IV. Risk Management Functions; and
- V. Activities considered illegal under any law in The Gambia

14. The Bank would not support the outsourcing of the above-mentioned activities as these are an integral part of systems that provide integrity and effectiveness of controls mechanisms established and maintained by Management. However, exceptions for certain types of intra-group outsourcing may be allowed with the Bank's approval, this would be considered on a case-by-case basis. Financial institutions that intend to outsource the aforesaid activities within the group, are required to seek prior authorization of the Bank.

#### Outsourcing Outside The Gambia ("Offshoring")

15. Financial institutions may undertake outsourcing activities to service providers outside The Gambia, also known as 'offshoring'. This practice increases the exposures of a financial institution to country risk. Financial institutions that engage in cross-border outsourcing should consider the country risk element hence, the capacity or ability of the service provider to deliver the service uninterruptedly. They should avoid cross-border outsourcing arrangements with countries that do not have legislation on

confidentiality and where regulators may be denied access to information held by such service providers.

16. Financial institutions should also consider scenarios in case of disruptions in business continuity. An aspect that a financial institution should consider seriously in this respect, is how quickly and efficiently the processes could be reverted to the home country to keep to a minimum potential disruption of service by the financial institution due to this factor.

17. Offshoring is permissible only if the goods and services are not available locally - in the country.

#### 18. Intra-Group

Financial institutions intending to enter into an outsourced activity with their group or a related party should follow risk management practices such as:

- Ensure that the activity to be outsourced with the group or its related party is indeed relevant to the financial institution and cannot be outsourced in the country.
- The cost involved should not hinder the activities or profitability of the financial Institution.
- Financial institutions considering undertaking outsourcing with their group or a related party should ensure that it does not in any way minimise or lessen the responsibilities of the board and senior management who have the overall responsibility and ultimate control of the outsourced activity.
- Financial institutions should consider all the relevant laws and regulations, guidelines and approval conditions within The Gambia and the country the group is resident or its related party.
- Financial institutions need to ensure and demonstrate that the agreements entered with parent groups or related entities are done at arm's length.

## Cloud-based Services

19. The Bank considers cloud-based services operated by service providers as a form of outsourcing and recognises that financial institutions may have recourse to such services to enhance their operations and service efficiency. The usage of cloud-based services by financial institutions shall be restricted to non-core activities only.

20. Cloud-based services are subject to the same types of risks as in other forms of outsourcing arrangements. Financial institutions should, therefore, perform the necessary due diligence and apply sound governance and risk management practices when subscribing to cloud-based services.

21. The Bank expects Financial institutions to be fully aware of cloud-based services characteristics such as multi-tenancy, data commingling, and the possibility for processing to be carried out in different locations. Financial institutions are required to take appropriate measures with respect to data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. They should ensure that the service providers have the capacity to identify and segregate customer data using strong physical or logical controls.

22. Financial institutions are ultimately responsible and accountable for maintaining oversight of cloud-based services and managing the attendant risks of adopting cloud-based services, as in any other form of outsourcing arrangement.

23. The implementation of cloud-based services by financial institutions would be subject to the following conditions:

- i. The Board of Directors of a financial Institution shall approve the adoption of cloud-based services and the exit mechanism of the outsourced facility.
- ii. The financial institution should have recourse to private or hybrid clouds for hosting applications with sensitive data. Public clouds may be used, subject to the authorisation of the Board of Directors of the financial institution

- provided that the customer data resides on private clouds. Under no circumstances should data be stored on personal, free or community-based cloud storage services such as Dropbox™, OneDrive™, GoogleDrive™, etc.
- iii. Financial institutions should ensure that data on the cloud and the channel to access them are encrypted. The encryption key should be retained by the financial institution.
  - iv. Financial institutions should, at the time of seeking approval from their Board of Directors, ensure that they are in possession of a certificate of conformity from a law practitioner, certifying that the systems in place comply with data protection laws and other applicable statutes in The Gambia and/or their country of domicile.
  - v. The cloud service provider should have a proven track record of at least three years.
  - vi. The cloud systems in place should demonstrate full business continuity and fall-backs. The functionality of a financial institution should not be affected due to possible disruptions in the system. The financial institution must implement proper business continuity planning in case the main access is not available.
  - vii. On a yearly basis, the financial institution should provide to the Bank a certificate of comfort from an independent reputable IT firm, certifying, inter-alia, compliance with the cloud-based services requirements set out in this guideline. All systems, processes and risk management practices should be well in place for the adoption of cloud technologies. The IT firm should conduct appropriate penetration tests to verify the security arrangements. The results of regular penetration tests should be annexed to the certificate of comfort.
  - viii. The authorities of the country in which the cloud servers would be kept and the cloud service providers should not by any means, have access to the data of the financial institution.
  - ix. Financial institutions should include a clause in the agreements with their cloud service providers, authorising the Bank or any firm authorised by the Bank to carry out examinations at the cloud servers/data centres, at any time.
  - x. Financial institutions should demonstrate that there would be a proper exit mechanism in place to provide for the deletion of all data stored on the cloud servers, in the event they switch to another service provider or stop the service for any other reason. This arrangement should be included in the contract with

the cloud service provider. The Bank should have the assurance that data would be erased from the cloud in these circumstances. Further, there should be a quick mechanism for prompt erasure of data in the case of the closure of a financial institution.

## C. MANAGEMENT OF OUTSOURCING RISK

### Outsourcing Management Plan

24. A financial institution shall assess the effect of outsourcing on its overall risk profile and its exposure to the various risks before it executes an outsourcing contract and shall update this assessment periodically. The assessment shall include, *inter alia*, reference to the following risks:

- I. Compliance risk is an element of operation risk that comes about when the service provider causes the financial institution to violate legal and regulatory requirements;
- II. Concentration risk, while normally considered important as an element of credit risk may also be an operational risk caused when a small number of service providers delivers a range of products and services to the financial institution or when several service providers are in the same geographical area;
- III. Reputational risk occasioned by faulty performance on the part of the service provider;
- IV. Country risk, also often considered a credit risk is an element of operational risk that arises when the service provider is located abroad and, for this reason, exposes the financial institution to political, economic, social, legal, and regulatory events in the country in which it is located;
- V. Operational risk, occasioned by a failure on the part of the service provider, including information-security failure, infringement of customers' privacy, and the eventuation of cyber risks;

VI. Legal risk and/or conduct risk brought about when a service provider exposes the financial institution to potential claims, e.g., claims by customers on grounds of unfair or illegal treatment.

25. A financial institution shall prepare and periodically update a comprehensive plan for the management of the risks that originate in outsourcing. The plan shall include a risk-minimization, monitoring and control of each outsourcing contract, including designating someone to be in charge, and guidelines for actions to be taken when certain events come to pass. In formulating the plan, the extent and materiality of the outsourced activity along with the quality of the service provider's risk-management shall be borne in mind.

26. The level of materiality of an outsourced activity shall be determined, *inter alia*, based on the following considerations:

- I. The extent to which a failure on the service provider's part will affect the financial condition, reputation and operations of the financial institution;
- II. Potential damage to customers of the financial institution in the event of a failure on the service provider's part.
  
- III. The effect of outsourcing on the financial institution's ability to comply with legal and regulatory requirements.
- IV. The costs of the outsourcing;
- V. The alignment of the outsourced activities with other activities undertaken within the framework of the financial institution;
- VI. The overall matrix of relations between the financial institution, as well as with the banking group to which it belongs, and a service provider that is not part of the banking group, including it being a "related person."
- VII. The service provider is abroad, or the financial institution's databases are sent or are stored abroad;
- VIII. The service provider's statutory status, including the level of supervision that applies to it;
- IX. The level of difficulty, including the costs of switching to another service provider, the time required to replace the service provider, the transfer

of all activity back to the financial institution, and the downscaling or even the discontinuation of activity, if necessary;

- X. The level of complexity of the contract with service providers, including cases in which several service providers collaborate to provide outsourcing services in respect of a certain activity;
- XI. The financial institution's ability to maintain adequate internal controls and comply with supervisory requirements, particularly when problems with the service provider arise;
- XII. The overall potential impact on the financial institution of a situation in which one service provider provides the same Financial Institution with several services; and/or
- XIII. The existence of a new product or service in the outsourced activity.

27. The financial institution shall establish methods for the measurement of the service provider's performance and shall appoint staff that has enough expertise and status to supervise their level of performance and determine the frequency and scope of the administrative reports that will be used to monitor and evaluate the service provider.

#### Business-Continuity Plan

28. A financial institution must be prepared for scenarios that may cause it significant disruptions. Viz:

- I. shall put together a business-continuity plan, including recovery from disaster, for each material outsourcing contract, and shall test it, inter alia, by means of periodic trials;
- II. shall make sure that said business-continuity plan relates to alternative ways of carrying out the activity as well as their costs, e.g., replacing a service provider, returning all activity to the financial institution, and downscaling and even discontinuing the activity;
- III. shall determine appropriate steps to deal with the potential outcomes of disruption of business due to the service provider's fault;

- IV. shall make sure that the service provider has a business-continuity plan in place and shall coordinate this plan with its own; said plan shall include, *inter alia*, documentation of those responsible for dealing with and preparing for situations of recovery from disaster, both at the financial institution and at the service provider, in accordance with the requirements of the Guideline;
- V. shall make sure that the business-continuity plan responds adequately to a failure of the service provider's information systems that may impair the financial institution's information security.

## Risk Management Framework in Outsourcing

### Policy Formulation

29. Prior to the outsourcing of any activity, a financial institution should establish a comprehensive policy on outsourcing, which should be approved by its Board. The policy should guide the assessment of whether and how an activity should be outsourced. The policy should be well documented and should include, *inter-alia*:

- I. Strategic goals, objectives and business needs of a financial institution in relation to outsourcing;
- II. A clear definition of the range of activities that may be outsourced and those core activities which cannot be outsourced;
- III. Steps to evaluate whether an activity is appropriate for outsourcing;
- IV. Criteria for determining material outsourcing;
- V. Processes for evaluating risks associated with an outsourced activity;
- VI. Criteria for evaluating outsourcing relationships (with service providers) including necessary controls and reporting processes on an ongoing basis;
- VII. Limits on the acceptable overall level of outsourced activities;
- VIII. Eligibility criteria for selecting service providers considering any relation, directly or indirectly, with the service provider;
- IX. Issues addressing risk concentrations and risks arising from outsourcing multiple activities to the same service provider;
- X. Steps to ensure compliance with legal and regulatory requirements in both home and host countries; and
- XI. Contingency plan in case of business disruptions.



## Role of the Board of Directors and Senior Management

30. The Board of Directors and Senior Management of a financial institution have the responsibilities for ensuring that an effective risk management system for outsourcing is in place.

The Board of Directors shall, as a minimum, be responsible for:

- I. Approving the policy on outsourcing;
- II. Assessing outsourcing strategies and arrangements to evaluate consistency with strategic objectives;
- III. Assessing how the outsourcing arrangement will support the financial institution objectives and strategic plans;
- IV. Laying down the appropriate approval authorities for outsourcing;
- V. Approving material outsourcing arrangements;
- VI. Approving the exit mechanism in respect of material outsourcing arrangements;
- VII. Assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures to commensurate with the nature, scope and complexity of the outsourcing arrangements;
- VIII. Reviewing all material outsourcing activities and relevant reports on outsourcing at least once annually;
- IX. Ensuring the continued maintenance of an overall framework for the operational stability of the Financial institution, considering the scope of outsourced services.

Senior Management has the responsibility for proper management of the risks associated with outsourcing activities. In addition, senior management is responsible for:

- I. Evaluating the risks and materiality of outsourcing activities;
- II. Developing and 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 authorities to assess any outsourced functions; and
- VII. Ensuring that regulatory and legal requirements are always complied with, in the framework of outsourced services.

#### Evaluation of Risks Involved in Outsourcing

**31.** The responsibility for implementing a risk management framework on outsourcing lies with the management. The Board of Directors and Management should, always have a full understanding of the various risks associated with outsourcing. The risk management on outsourcing should include, inter-alia, the following steps:

- I. Identification of the role of outsourcing in the overall business strategy;
- II. Due diligence on the service provider and effective identification of the key risk mitigation strategies;
- III. Analysis of the impact of the outsourcing arrangement on the overall risk profile of the financial institution; and
- IV. Analysis of risk-return on the potential benefits of outsourcing.

#### Due Diligence in Selecting Service Providers

**32.** Financial institutions are required to carry out stringent due diligence in selecting service providers. They should develop criteria that would enable them to select service providers, both within and outside The Gambia, that have the capacity and ability, both operationally and financially, to perform the outsourced activities. The due diligence exercise, based on updated information, should be duly documented, and should include as a minimum, an assessment of:

- i. The experience and competence of the service provider to implement and support the proposed activity over the contracted period;
- ii. The reputation of the service provider in respect of the services offered, the quality and dependability of its personnel;
- iii. The financial soundness of the service provider to fulfil its obligations, based on updated audited financial statements;
- iv. The internal control systems, audit coverage, compliance, reporting and monitoring environment, system development and maintenance, insurance coverage, and ability to respond and the speed of response to service disruptions by the service provider;
- v. The commitment of the key service provider personnel towards compliance with rules and regulations to which the outsourcing financial institution is subjected;
- vi. The capability to offer service support to ensure continuity of operations at the financial institution and the reliance of service providers on sub-contractors and other parties; and
- vii. The existence, at the service provider's level, of a process for business continuity management.

**33.** Financial institutions should pay periodic on-site visits to the service provider to better understand and develop the necessary confidence as to the way the service provider operates and supports its services.

**34.** Financial institutions intending to engage in outsourcing from abroad should, in addition to Section 16, carry out an assessment of the economic, legal and political environment in which the service providers operate.

#### **Contract Issues & Service Level Agreement**

**35.** Outsourcing arrangements between financial institutions and service providers should be governed by formal and comprehensive written contracts. Contracts should clearly spell out the rights and responsibilities of each party, taking into consideration the specificities and the materiality of the outsourced activities.

36. The agreement should not consist of clauses that would hinder the Bank from exercising its supervisory powers. The Bank should have the same right of access to information with the service provider as it has with the financial institution having undertaken the outsourcing. The contract should explicitly allow for on-site visits and unhindered inspections of the outsourced activities by the financial institution and the Bank.
37. The agreement should consist of a clause for seeking the prior approval of the Bank in the event of sub-contracting of material activities which have been outsourced by a financial institution to any other entity.
38. Other provisions to be included in an outsourcing contract are:
- I. the scope of the outsourcing activities, including clear definitions of functions to be outsourced to the service provider as well as the timeframe for implementation;
  - II. cost and maintenance;
  - III. confidentiality and security;
  - IV. contingency planning in the event the service provider fails;
  - V. access of the financial institution and the Bank to all books, records and information relevant to the outsourced activity provided by the service provider;
  - VI. continuous monitoring and assessment by financial institution of the service providers;
  - VII. types of audit reports and other reports that financial institution should receive, for example, audited financial statements and performance reports;
  - VIII. reporting of any material weakness that may impact negatively on the financial soundness of the service provider, to the concerned financial institution;
  - IX. Dispute resolution;
  - X. A termination and early exit clause in case of default by the service provider, including insolvency, liquidation, receivership, change in ownership;

- XI. Conditions of subcontracting by the service provider for all or part of an outsourced activity and contingency planning for business resumption;
- XII. the need, if any, for insurance cover to be contracted by the service provider;
- XIII. In case the service provider is located outside The Gambia, choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.

**39.** Moreover, financial institutions should ensure that a service level agreement is put in place when entering an outsourcing arrangement with a service provider. The service level agreement should contain a mixture of quantitative and qualitative performance targets, to enable the outsourcing institution to assess the adequacy and effectiveness of service provision.

**40.** Any outsourcing agreement shall not affect the rights of customers towards the financial institution, including their ability to obtain redress.

**41.** The Bank may, in the light of any adverse information, direct a financial institution to modify, review or terminate an outsourcing arrangement in the interest of its customers or any other stakeholder.

#### **Contingency Planning**

**42.** Financial institutions should take appropriate steps to assess and address the potential consequences in case of a business disruption of an outsourced activity. They should ensure that necessary contingency plans are in place for business continuity in the event the service provider fails, or the contract terminates prematurely or there is non-performance on the part of the service provider. Each outsourcing arrangement should be accompanied by relevant contingency plan.

43. Contingency plans should address issues such as availability of alternative service providers and hand-over process to a new acceptable supplier. The plans can also be related to worst-case scenarios.

44. Financial institutions should test and review their contingency plans pertaining to the outsourced activities on a regular basis.

#### Confidentiality and Security

45. Outsourcing agreements should contain a clause that would address the service providers' responsibility for confidentiality and security. Financial institutions that engage in outsourcing should take appropriate steps to protect confidential customer information. Financial institutions should expressly prohibit service providers from disclosing confidential customer information to any third-party except for regulatory purposes.

46. Depending on the nature and materiality of the outsourcing arrangement, financial institutions should consider the possibility of notifying in advance their customers that customer data may be transmitted to a service provider as part of their contractual arrangement with the customers.

47. A Financial Institution should report to the Bank immediately about any unauthorised access or breach of confidentiality and security, directly or indirectly, by an outsourced service provider and the action/s it is proposes to take in consequence.

#### Role of the External Auditor

48. The external auditor should review and attest the adequacy of the policies and processes put in place by financial institution for outsourcing activities. They should immediately inform the Bank of any material weaknesses or irregularities that, in their opinion, might affect the well-being of the financial institution or have additional operational risk implications.

#### Application of the Guideline

49. This Guideline is applicable to all financial institutions falling under the regulatory purview of the Bank. It needs to be emphasized that financial institutions should seek prior authorization of the Bank before embarking on both material and non-material outsourcing.

50. Financial Institutions should assess all their existing (both material and non-material) outsourcing arrangements against this Guideline. Where there are challenges, a financial institution shall submit a request to the Bank in writing, for a case-by-case review. Moreover, a plan and timeframe on how such weaknesses would be rectified would be outlined and this should be done within 4 months from the effective date of this Guideline.

51. Financial institutions should inform the Bank immediately, of any adverse development arising from any outsourcing arrangement that could significantly affect their businesses.

#### Annual reporting

52. On a yearly basis, financial institutions should submit to the Bank a Return on outsourced activities, containing a list of all material and non-material activities that have been outsourced, in such form and manner prescribed by the Bank.

This return should be submitted within the next twenty working days of the start of the ensuing calendar year.

#### D. REGULATORY PROCESS

##### Approval for outsourcing arrangements

53. A financial institution must obtain the Bank's written approval before—
- I. Entering a new material or non-material outsourcing arrangement; or
  - II. Making a significant modification to an existing material outsourcing arrangement.

54. In assessing an outsourcing application, the Bank will have regard, among others, to the following factors:

- I. The state of controls, risk management and governance of the financial institution;
- II. The materiality of the outsourcing arrangement;
- III. Other relevant matters, including any cooperation arrangements between the Bank and relevant financial regulatory authorities.

55. An application for approval pursuant to paragraph 8.1 must comprise, at a minimum, of the following information:

- I. Name and registered address of the service provider, including the sub-contractors, where applicable;
- II. Date of commencement of the arrangement and expiry or renewal date;
- III. A brief description of the activity to be outsourced;
- IV. The locations (e.g. City and country) where the outsourced activity is undertaken by the service provider and sub-contractors, including where information is processed or stored, and the primary and back-up locations;
- V. Where the arrangement involves the use of cloud service providers, the cloud Services, deployment model, nature of data to be held and locations (e.g. City and Country) where such data is stored, including back-up locations;
- VI. Outcomes of the financial institution's due diligence process on the capacity of the service providers;
- VII. Aggregate exposure to a particular service provider in cases where the financial institution outsources various functions to the same service providers
- VIII. Total costs of the outsourcing arrangement, including upfront and ongoing expenses;
- IX. Financial information to include but not be limited to the following:
  - i. Last three years' financial statements;
  - ii. Copy of last three years' financial audit; and
- X. All ownership details to the level of beneficial ownership;



- XI. In the case of an IT service provider, the application must be accompanied by
  - i. Business Continuity Plan
  - ii. Disaster Recovery plan including Recovery Site and testing frequency.
  - iii. Most recent IT audit including penetration testing results.
- XII. Detailed Cost Benefit analysis of requested outsource project.
- XIII. Overall impact of the outsourcing arrangement on headcount and capacity within the Financial Institution;
- XIV. Evidence of the approval granted by the relevant approval authority as determined under the Financial Institution's internal governance framework.

#### Sanctions for Non-compliance

**56.** Failure to comply with the provisions of this Guideline shall attract a penalty of 5 percent of the outsourcing arrangement cost.

**57.** Guiding Principles on Outsourcing of Financial Services as developed by the Joint Forum of the Basel Committee on Banking Supervision may be referenced for further information.