BANK OF GHANA

OUTSOURCING DIRECTIVE

FOR BANKS, SPECIALISED DEPOSIT-TAKING INSTITUTIONS, FINANCIAL HOLDING COMPANIES AND DEVELOPMENT FINANCE INSTITUTIONS

EXPOSURE DRAFT

DECEMBER 2023

The Bank of Ghana (BOG) has issued the Outsourcing Directive as an **Exposure Draft** to solicit comments and inputs from the banking industry and the general public, in line with the BOG's Procedures for Issuance of Directives, 2020.

In light of this, the Exposure Draft shall be made available on the BOG's website at www.bog.gov.gh for a period of not less than fourteen (14) days from the date of the publication of the Exposure Draft, for comments.

All comments shall be sent to the Bank of Ghana via email at bsdletters@bog.gov.gh by 31st January 2024. The Bank of Ghana shall consider all material comments received and provide a written explanation for comments that were incorporated into the final directive or otherwise.

INTRODUCTION

In recent years, there has been an increasing tendency by banks and specialised deposit-taking institutions (SDIs), herein referred to as regulated financial institutions (RFIs), to outsource activities to reduce costs and improve efficiency.

Empirical data indicates that outsourcing in the banking sector was initially limited to activities that did not pertain to institutions' primary business, such as payroll processing. More recently however, commonly outsourced activities have included information technology (IT), management services, accounting, audit, and human resources, among others.

In the context of digitalisation and the increasing importance of IT and financial technologies (FinTech), RFIs are adapting their business models, processes, and systems to embrace such technologies. IT has become one of the commonly outsourced activities in the banking sector. Notwithstanding its benefits, outsourcing IT and data services presents information security risks and challenges to the governance framework of RFIs, in particular, to internal controls as well as to data management and data protection.

The Bank of Ghana (BOG) recognises that RFIs may have sound reasons to outsource functions, such as the ability to achieve economies of scale or to improve the quality of service to customers, or to improve the quality of risk management. The main reasons for outsourcing are to reduce and control operating costs and to meet the challenges of technological innovation, increased specialization, and heightened competition. RFIs have intensified the use of IT and FinTech solutions and have launched projects to improve their cost efficiency.

The outsourcing of business activities can however increase the RFI's dependence on service providers which may heighten its risk profile and jeopardize overall safety and soundness, particularly where material business activities, services or processes are outsourced to an unregulated third party or an overseas service provider.

Outsourced services are also becoming increasingly complex and may increase an institution's exposure to strategic, reputation, compliance, operational, country and concentration risks. Consequently, the BOG has issued this Directive to RFIs to ensure that they effectively manage the risks associated with outsourcing activities.

In view of the foregoing, the BOG will consider the impact of the outsourced services when conducting a risk assessment of an RFI. The assessment will include inter alia a determination of whether the outsourcing arrangement hampers in any way the RFI's ability to meet its regulatory requirements.

The BOG will consider the potential systemic risks posed where outsourced activities of multiple regulated entities are concentrated in a single or limited number of service providers.

Outsourcing must not lead to a situation where an RFI becomes an 'empty shell' that lacks the substance to remain licensed. To this end, the Board and Senior Management should ensure that sufficient resources are available to appropriately support and ensure the performance of their responsibilities, including overseeing the risks and managing the outsourcing arrangements.

Table of Contents

PART I - PRELIMINARY

Title

1. This Directive may be cited as the **Bank of Ghana Outsourcing Directive, 2023**

Application

2. This Directive is issued under the powers conferred by Section 92 of the Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930) as well as Section 84 of the Development Finance Institutions Act, 2020 (Act 1032) and shall apply to all banks, Specialised Deposit-taking Institutions (SDIs), Financial Holding Companies (FHC), and Development Finance Institutions (DFIs) collectively referred to in this Directive as "Regulated Financial Institutions (RFIs)".

Interpretation

3. In this Directive, unless the context otherwise requires, words used have the same meaning as that assigned to them in the applicable law (e.g., Act 930) and other Directives issued by the BOG or as follows:

"Act 930" *means the Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930);*

"Act 1032" *means the Development Finance Institutions Act, 2020 (Act 1032);*

"Bank" *means a body corporate which engages in the deposit-taking business and is issued with a banking licence in accordance with Act 930;*

"BOG" *means Bank of Ghana;*

"Cloud Computing" *means a model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service,*

ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).
a significant business function, process, service, or activity that is considered critical or material to the RFI's business model or strategy;

"Core Function" *means a significant business function, process, service, or activity that is considered critical or material to the RFI's business model or strategy;*

"Development Finance Institution" *means an institution (a) licensed under Act 1032 to carry out development finance business or (b) designated as a development finance institution by the Bank of Ghana by notice and published in the Gazette;*

"Financial Group" *means a corporate group that includes a bank or a specialized deposit-taking institution and its affiliates or associates that the Bank of Ghana determines to be taken into account for the purposes of Act 930;*

"Financial Holding Company" *means a company that controls a bank or specialised deposit-taking institution which is subject to the registration requirements of Act 930;*

"Foreign Bank" *means a foreign company that is authorised to engage in a deposit-taking business in the country where its head office is located;*

"Foreign Company" *means a company incorporated under the laws of a country other than Ghana;*

"Function" *means a* process, service or activity that is ordinarily undertaken by an RFI in the normal course of business;

"Insider" *means* a director, an executive director, key management personnel and a significant shareholder other than a financial holding company;

"Intra-group outsourcing" *means outsourcing a function to an entity within the same financial group or group structure (an affiliate) - common ownership;*

"Immaterial" *means a function that does not have a significant impact on the RFI's ability to meet its legal/regulatory requirements, obligations to customers, reporting requirements, financial performance or continue its business operations or the effectiveness of internal controls;*

"Material" *means a function of such importance that any defect, weakness or service failure or security breach has the potential to significantly impact on the RFI's ability to meet its legal/regulatory requirements, obligation to customers, reporting requirements, and impacts financial performance and effectiveness of internal controls or the RFI's ability to continue its business operations;*

"Non-Core Function" *means an immaterial function that is considered peripheral or incidental to the RFI's business model or strategy;*

"Outsourcing" *means* an arrangement of any form between an RFI and a service provider by which the service provider performs a function that would otherwise be undertaken by the RFI itself;

"Outsourcing Agreement" *means an agreement between an RFI and a service provider (includes its sub-contractors) by which the service provider performs a function that would otherwise be undertaken by the RFI itself;*

"Non-Outsourcing Third-Party Agreement" *means an agreement between an RFI and a third party (refers to either an affiliated entity within a group or an entity external to the group) whereby the third party performs a function on a non-continual basis;*

"Person" *includes an individual, a body corporate, a partnership, an association, and any other group of persons acting in concert, whether incorporated or not;*

"Regulated Financial Institution (RFI)" *means a bank, a specialised deposit-taking institution, a financial holding company or a development finance institution covered under this Directive;*

"Security Operations Centre (SOC)" *means the facility where all ICT equipment, applications, infrastructure, data centre, network, and all endpoints are monitored, assessed and defended and is related to people, processes and technology involved in providing detection, containment and remediation of IT and cyber threats;*

"Senior Management" *means members of the Executive Management Committee (EXCO) of an RFI and any other Key Management Personnel (KMP)as may be determined by the Regulated Financial Institution;*

"Service Provider" *means a natural or legal person (including a parent bank or holding company and their related entities), domestic or foreign, that carries out outsourced processes, services or activities on behalf of an RFI. Such a person may be regulated or unregulated; and*

"Specialised Deposit-Taking Institution" (SDI) *means a body corporate which engages in the deposit-taking business and is issued with a licence to engage in the deposit-taking business in accordance with Act 930;*

"Strategic Function" *means a core function that cannot be outsourced since they are the core Board and Management responsibility /function and include strategic oversight, risk management, internal audit, and compliance functions (Annexure II);*

"Non-Strategic Function" *means a core function that requires prior written approval from the Bank of Ghana before being outsourced and include human resource and back-office management (Annexure I); and*

"Sub-Contractor" *means a person, including an affiliate, which performs or assists in performing the whole or part of the outsourced function for the primary service provider covered under the outsourcing agreement.*

Prior Approval Requirement

4. In accordance with Section 60 (12) of Act 930 or Section 57 (12) of Act 1032, an RFI shall not outsource a function/ core function to any other person without the written prior approval of the Bank of Ghana.

Proportionality

5. RFIs are required to fully comply with this Directive. However, the BOG having regard to the principle of proportionality would ensure that the application of proportionality aims to ensure governance arrangements, including those related to outsourcing, are consistent with the systemic importance, risk profile, nature and business model of the RFI , and the scale and complexity of their activities so that the objectives of the regulatory requirements are effectively achieved. When applying the requirements set out in this Directive, RFIs shall consider the complexity of the outsourced function, the risks arising from the outsourcing arrangement, the materiality of the outsourced function and the potential impact of the outsourcing arrangement on the safety and soundness of the RFI.

Supervisory Approach

6. As outsourcing of functions can bring significant benefits to RFIs and their customers, the BOG will not stand in the way of RFIs using outsourcing arrangements to achieve their business objectives, provided that such arrangements are well-structured and adequately managed, and the interest of depositors are not compromised.

7. For outsourcing to an offshore service provider, the BOG may also communicate directly with the RFI's home or host supervisors/authorities to seek confirmation on various matters.

8. Once an RFI implements an outsourcing plan, the BOG expects the RFI to continue to review the effectiveness and adequacy of the controls in monitoring the performance of the service provider and its sub-contractor and managing the risks associated with the outsourced function.

9. Where there are deficiencies in any outsourcing arrangements, the RFI should take appropriate action to rectify them, failing which the BOG reserves the right, in extreme cases, to require the RFI to take steps to make alternative arrangements for the outsourced function.

10. RFIs are required to submit to the BOG, their materiality assessment framework for approval and the BOG may invite the RFI for further engagements. RFIs are also required to keep records of all materiality assessments and the relevant analysis and outcome together with a list of all immaterial or non-core functions that the RFI has outsourced. The RFIs shall also make these assessments available to BOG whenever requested. The BOG shall review these records as part of its supervisory review process and shall take appropriate supervisory action where gaps are identified.

11. The BOG will, in the course of its on-site examinations, off-site monitoring, or prudential interviews with RFIs, establish whether outsourcing risks have adequately been addressed. The BOG will review RFIs' implementation of this Directive, the quality of its Board and Senior Management oversight and governance, internal controls, and risk management regarding effectiveness of managing outsourcing risks to identify gaps for corrective action/supervisory intervention by the BOG.

12. As part of its ongoing supervisory activities, the BOG shall assess the strength of the RFI's oversight and internal controls pertaining to its outsourcing arrangements and shall determine whether the RFI is exposed to undue risk without appropriate risk mitigants in place. Where internal controls or governance weakness are identified or where the risks from outsourcing arrangements are assessed as being excessive without corresponding mitigants in place, BOG shall take appropriate supervisory actions which may include requiring the RFI to implement specific measures to address the identified deficiencies or, in extreme, requiring the RFI to review the outsourcing arrangements with the service provider.

Objectives

13. Objectives of the Directive are to:

    a. Operationalise section 60 (12) of Act 930 and section 57 (12) of Act 1032 pertaining to outsourcing arrangements;

    b. Provide guidance on regulatory requirements regarding outsourcing arrangements;

    c. Ensure that outsourcing arrangements neither diminish RFIs' ability to fulfil its obligations to customers nor impede effective supervision by the BOG;

d. Ensure that material outsourcing arrangements with service providers and their sub-contractors do not pose excessive risk to RFIs

e. Provide a framework which guides RFIs in all outsourcing arrangements to ensure that:

i. material outsourcing arrangements entered into by an RFI are subject to appropriate due diligence, approval, and on-going monitoring and supervision;

ii. expectations of the BOG are set out regarding risks arising from outsourcing arrangements by an RFI are appropriately managed to ensure that an RFI can meet its financial and service obligations to customers, and other stakeholders;

iii. dealings between the RFI and outsourced service providers are conducted at arm's length.

Transitional Arrangements

14. RFIs which have existing outsourcing contracts in place that do not meet the requirements in this Directive are required to:

a. Review those contracts and ensure compliance with this Directive the earlier of either the renewal date of the contract or by 30th June 2024; and

b. Notify the BOG within three (3) months of the issuance of this Directive of the following:

i. All existing outsourcing contracts using Annexure VIII; and
ii. Material outsourcing contracts identified in (i.) above which do not comply with this Directive and the areas of non-compliance as well as a plan, including a timeframe within which to address the weaknesses or deficiencies.

15. RFIs shall not require the prior written approval of the BOG to enter into an outsourcing arrangement pertaining to a non-core function provided the function does not require approval under any other provision of Act 930 or any other legislation. However, the RFI shall notify the BOG ten (10) days prior to engaging the service provider.

16. All new proposed outsourcing arrangements, including renewals, amendments and extensions of contracts or outsourcing agreements, for a

core function shall require the Bank of Ghana's prior written approval as per section 60 (12) of Act 930.

17. This Directive shall not apply to functions not considered under outsourcing arrangements as provided in Annexure IV.

18. The effective implementation date of this Directive shall be **1st July 2024.**

PART II – GOVERNANCE AND RISK MANAGEMENT FRAMEWORK FOR MATERIAL OUTSOURCING ARRANGEMENTS

Governance

19. In any outsourcing arrangement, the Board and Senior Management of an RFI shall retain ultimate accountability for the outsourced function. Outsourcing can only allow the Board and Senior Management to transfer their day-to-day managerial responsibility, but not accountability. It is important for RFIs to recognise that outsourcing a function does not transfer all of the risks associated with the function to the service provider and its sub-contractor. It remains the responsibility of the RFI to ensure that all risks associated with the function are addressed to the same extent as they would be if the function was performed "in house". RFIs should therefore continue to retain ultimate control of any outsourced function.

20. **The Board** of an RFI or a committee delegated by it shall be responsible for:

    a. ensuring that an RFI has in place an outsourcing policy to ensure its ability to oversee effectively the function being outsourced;

    b. maintaining effective oversight of the RFI's outsourcing arrangements;

    c. setting a clear and suitable risk appetite to define the nature and extent of risks that the RFI is willing and able to assume from its outsourcing arrangements, including risk concentration arising from outsourcing multiple functions to a single service provider;

    d. assessing how the outsourcing arrangement will support the RFI's objectives and strategic plan;

    e. approving the outsourcing risk management framework and policies to:
        i. assess and manage the exposure of RFI to risks due to outsourcing arrangements on an on-going basis;
        ii. assess the materiality of functions to be outsourced to facilitate distinction between core and non-core functions; and
        iii. include relevant due diligence processes, vendor management and risk assessment criteria whilst ensuring that the minimum contractual agreement requirements are adhered to.

    f. approving all material outsourcing arrangements;

    g. setting clear roles and responsibilities of the Board and Senior Management including personnel or organisational functions that will be responsible for oversight of the RFI's outsourcing arrangement;

h. ensuring that Directors possess adequate understanding of outsourcing risks and key management personnel are equipped with appropriate expertise for managing such risks;

i. obtaining written approval from the BOG prior to outsourcing of any core function;

j. ensuring effective management and monitoring of outsourcing risks and establishing adequate risk mitigants, including appropriate and effective business continuity and contingency planning, for outsourcing arrangements and exit plan to ensure that RFIs recover from outage or failure of a service provider and, if necessary, exit from the outsourcing in a way that minimizes potential disruption[1];

k. ensuring that senior management establishes appropriate governance structures and processes for sound and prudent risk management, such as a management body that reviews controls for consistency and alignment with the RFI's view of risk;

l. undertaking regular reviews and monitoring of the outsourcing strategies and arrangements for their continued relevance, to support safety and soundness;

m. establishing a sound internal governance structure that provides effective oversight and control over outsourcing arrangements, consistent with the RFIs overall business strategy and risk appetite;

n. retaining sufficient management capacity and skilled resources within the institution to oversee the outsourced activity, including where the outsourced activity is undertaken by an affiliate of the RFI, the Board shall put in place adequate processes to ensure that:

   i. the outsourcing arrangement does not create situations of conflict between the RFI and the service provider and/ or sub-contractors;
   ii. the RFI retains the continuous ability to comply with regulatory and supervisory requirements; and
   iii. outsourcing arrangement is conducted on an arms-length basis.

o. ensuring that the group-wide outsourcing risk management framework adequately addresses outsourcing risk across entities within the group, where an RFI is responsible for oversight over its subsidiaries.

[1] An effective business continuity plan should ensure that an RFI can recover from an outage or failure of a service provider within a reasonable time.

21. **Senior Management** of an RFI shall be responsible for:

a. developing, implementing, monitoring and regularly reviewing the effectiveness of the outsourcing arrangement, risk management framework, policies, procedures, tools, and metrics;

b. evaluating the materiality and risks from all existing and prospective outsourcing arrangements, based on the framework approved by the Board;

c. establishing an internal escalation process for managing outsourcing risk and ensuring that appropriate and timely remedial actions are taken to address the risk;

d. allocating adequate resources with appropriate expertise and ensuring ongoing capacity building and training of staff on effective management of the RFI's outsourcing risk;

e. ensuring that the internal audit function and the external auditors have the authority and access to information to be able to adequately and promptly assess any outsourced function;

f. ensuring that there is independent review and audit for compliance with outsourcing regulations, policies and procedures;

g. keeping the Board informed on material outsourcing risks in a timely manner, including through regular reporting;

h. ensuring that regulatory requirements on outsourced activities are complied with at all times;

i. maintaining an up-to-date outsourcing risk register[2] or centralized list of all outsourcing arrangements with an identification of all core functions outsourced to a service provider;

j. ensuring that one internal unit, function or individual is identified as being responsible for the documentation, management, monitoring and control of each outsourced function or service, and proper and timely reporting to the Board and Senior Management;

[2] The risk register shall include, but not limited to the name of the service provider and sub contractors, short description of the arrangement, type of arrangement (intra-group/foreign service provider and country), expiry or renewal date, estimated annual spending, systemic importance (concentration of the service provider within the financial sector), and other items of note (e.g. non-compliance with performance measures, etc.).

k. managing the confidentiality of customer information and related requirements, monitoring the financial condition and operational capability of the service provider and, in the event the service provider fails or deteriorates, ensuring that business continuity arrangements are in place and reported to the Board on a timely basis;

l. Ensuring that contingency plans are based on realistic and probable disruptive scenarios and ensuring that these plans are periodically tested and updated, where necessary; and

m. developing feasible exit plan and carrying out analysis of the potential cost and timing of either transferring an outsourced service to an alternative service provider or reincorporating the service in-house.

22. The Board and Senior Management shall be ultimately accountable for any outsourced function and should therefore exercise the appropriate oversight over the service providers.

Risk Management

23. An RFI shall develop an outsourcing Risk Management Framework (RMF) to manage all outsourcing risks in a systematic and consistent manner in line with this Directive and in conjunction with BOG's Risk Management Directive, 2021, as well as Risk Management Guidelines for Rural and Community Banks, 2021 and shall include:

a. identifying the role of outsourcing in the overall business strategy and objectives of the RFI;

b. performing comprehensive due diligence on the nature, scope and complexity of the outsourcing arrangement to identify and mitigate key risks;

c. clear articulation of the roles and responsibilities of business lines and functions in managing outsourcing risk;

d. implementation of effective risk management practices and internal controls to manage outsourcing risk;

e. identification and assessment of outsourcing risk emanating from service providers and their sub-contractors as well as risks inherent[3] in the outsourced function;

[3] Inherent risks in the outsourced function shall, at a minimum, include strategic risk, reputation risk, compliance risk, operational risk, cyber risk, country risk, and concentration risk.

f. assessing a service provider and its sub-contractors' ability to employ a high standard of care in performing the outsourced function and meet regulatory standards as expected of the RFI as if the outsourcing arrangement is performed by the institution;

g. analysing the impact of the outsourcing arrangement on the overall risk profile of the RFI, and whether there are adequate internal expertise and resources to mitigate the risks identified;

h. analysing both the RFI's as well as the RFI's group aggregate exposure to the outsourcing arrangement, to manage concentration risk;

i. incident detection, response and reporting system as well as policies and procedures to detect activities that may impact on service provider's information security (including data breaches, incidents (including cyber incidents), or misuse of access by service providers) and respond to these incidents appropriately (including appropriate mechanisms for investigation and evidence collection and reporting after an incident);

j. effective ongoing monitoring of outsourcing risks and provision of timely update to the RFI's Board and Senior Management; and

k. policy on outsourcing risk management which should be approved and periodically (at least annually) reviewed by RFI's Board in light of changing circumstances and applicable laws to ensure that it is fit-for-purpose. The policy shall be consistent with the provisions of this Directive.

24. RFIs shall immediately inform the BOG of any adverse development pertaining to an outsourcing arrangement or outsourcing service provider that could negatively impact on the business or operation of the entity including but not limited to breaches of security or confidentiality of outsourced data.

25. RFIs shall have in place appropriate plans to ensure an orderly exit from outsourcing arrangements related to core functions where necessary by, migrating to another service provider or by reintegrating the core outsourced function.

26. The RFIs shall implement robust processes for:

    a. monitoring and mitigating risks posed by outsourcing of core functions to a dominant service provider that is not easily substitutable and multiple outsourcing arrangements with the same service provider or closely connected service providers;

    b. managing potential conflict of interest that could arise due to outsourcing arrangements including between entities within the same group; and

    c. addressing the risk that could result from the need to provide financial support to a service provider in distress or to take over its business operations.

27. RFIs shall develop, maintain and periodically test appropriate business continuity plans with regard to outsourced core functions[4]. Such plans should take into account: (i) the possible events that the quality of the provision of the outsourced core functions deteriorate to unacceptable levels or fails; (ii) the potential impact of insolvency or other failure of the service provider; and (iii) political/ country risk in the service provider's jurisdiction, where relevant.

28. RFIs shall have a documented exit strategy when outsourcing core functions that is in line with their outsourcing policy and business continuity plans, and which should take into account at least the possibility of: (i) termination of outsourcing arrangements, (ii) failure of the service provider, (iii) deterioration in the quality of the outsourced function , and (iv) material risks arising for the appropriate and continuous application of the function.

29. RFIs shall take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance, and auditing. RFIs should, in particular, ensure that service provider have: (i) the ability to clearly identify and segregate customer data, and (ii) robust access controls to protect customer information.

30. RFIs shall ensure that a service provider, if not a member of a group, shall **not** be owned or controlled by any significant shareholder, director, or key management personnel, or approver of the outsourcing arrangement of the RFI or their relatives.

[4] The business continuity plans, and business continuity exercises (test) should ideally be aligned with the expectation of the Basel Committee on Banking Supervision (BCBS) Principles of operational resilience (March 2021).

31. RFI should ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and regulators, nor impede effective supervision by the BOG**.**

Materiality Assessment

32. An RFI shall develop a basis for materiality assessment by which a function shall be considered as a ***core*** or ***non-core*** function.

33. An RFI shall develop a materiality assessment framework which shall be submitted to the BOG for approval following the RFI's Board approval. The BOG may require further engagement(s) with the RFI prior to the granting of its approval.

34. The materiality assessment shall be undertaken prior to entering into any outsourcing arrangement, with the end result being a determination of whether the outsourcing arrangement is considered a core or non-core function.

35. An RFI shall consult with the BOG, in writing, if after performing a materiality assessment based on the adopted methodology, it is not clear whether a function should be considered as core or non-core. Examples of core and non-core functions, though not exhaustive, are provided in Annexure I.

36. All outsourcing arrangements including non-core functions shall be added to the RFI's outsourcing risk register and the risk register submitted to BOG on a quarterly basis and whenever it is requested.

37. Notwithstanding the above, an RFI shall not outsource certain core functions which may affect the effective and efficient management of the operations of an RFI, if outsourced. These functions shall remain within the RFI in order not to lose control. Examples of core functions which ***shall not*** be outsourced are provided in Annexure II.

38. RFIs shall consider as part of its materiality assessment the following, among others:

    a. the impact of the outsourcing arrangement on the earnings, solvency, liquidity, funding, capital, ability to meet customers' obligations, reputation, operations of the RFI, or a significant business line, particularly if the service provider, or group of affiliated service providers, were to fail to adequately perform over a given period of time;

b. the ability of the RFI to maintain appropriate internal controls and meet regulatory requirements, particularly if the service provider experiences problems;

c. the cost of the outsourcing arrangements as a proportion of total operating cost of the RFI (a threshold of 5% or more of total operating costs is considered material);

d. the degree of difficulty and time required to find an alternative service provider or to bring the business activity in-house, if necessary;

e. the potential that multiple outsourcing arrangements provided by the same service provider can have a significant impact – in aggregate – on the RFI;

f. impact on RFI's customers, and counterparties should the service provider fail to perform the service or encounter a breach of confidentiality or security; and

g. cost to bring the outsourced activity in-house or to seek similar service from another service provider due to failure of the service provider (as a proportion of total operating cost of the RFI).

39. As minimum guidance, the BOG will consider an outsourcing arrangement material if:
    a. its annual payments to the service provider is 5% or more of its total operating cost;

    b. the service provider is given access to the RFI's general ledger or confidential customer information;

    c. an information security breach, other operational failure, or misconduct by the service provider and its employees and agents could plausibly lead to the RFI's inability to conduct a material line of business for more than 48 hours, or if the failure would plausibly lead to public exposure of confidential customer or counterparty information;

    d. the conservatively estimable cost of remediation of a service provider's inability to provide satisfactory performance exceeds the lesser of 5% of the RFI's Tier 1 capital, or 1% of the RFI's total assets;

    e. the revenue generated from that function to be outsourced is 5% or more of the RFI's gross income or the function to be outsourced forms 1% or more of the RFI's total assets (the lesser of the two);

f. a performance failure by the service provider could lead to long term impairment of the RFI's reputation, or the reputation of Ghana as a sound jurisdiction in which to conduct financial services; or

g. the outsourcing arrangement affects the RFI's ability to meet legal and regulatory reporting requirements.

40. Where an outsourcing arrangement with a service provider covers multiple functions, an RFI should consider all aspects of the arrangement with the materiality assessment.

41. An RFI shall undertake periodic reviews of its outsourcing arrangements to identify new outsourcing risks as well as materiality, as they emerge as outsourcing arrangement that was previously assessed as being immaterial may subsequently become material due to incremental services from outsourced service provider or change in nature of the outsourced service. Outsourcing risks may also increase due to sub-contracting by the service provider or significant changes to sub-contracting arrangements.

42. A list of sample questions to assess the materiality of outsourcing arrangements is provided in Annexure III.

Due Diligence Processes

43. In selecting a service provider, or renewing an outsourcing agreement, RFIs are required to undertake a due diligence process that appropriately assesses the risks associated with the outsourcing arrangement, including all factors that would affect the service provider's ability to perform the outsourced function.

44. An RFI shall carry out comprehensive due diligence in selecting service providers for outsourcing arrangements at the point of considering all new arrangements, and when renewing or renegotiating existing arrangements. The due diligence should be aimed at ensuring that the service provider has the ability, capacity and any authorisation required by law to deliver on the outsourced function in a satisfactory manner, considering the RFI's objectives and needs.

45. The due diligence process shall fully address the risks associated with the outsourcing arrangement and shall consider all the relevant features of the service provider, including qualitative (governance, operational and legal) and quantitative (financial) factors.

46. Factors to consider as part of an RFI's due diligence process shall include, but are not limited to, the following:

a. experience, capacity, and technical competence of the service provider to implement and support the outsourced function, which may include the review of the experience and technical competence of significant subcontractors where feasible;

b. financial strength and resources (e.g., most recent audited financial statements and other relevant information such as length of time in business, IT infrastructure);

c. corporate governance (including fitness and propriety of the shareholders and principals of the service providers), business reputation, ownership and group structure, complaints from customers, compliance with applicable laws and regulations including the required regulatory authorisations or registration, and pending or potential litigation;

d. internal controls, audit coverage, reporting and monitoring environment;

e. systems development and maintenance, security of systems and ability to meet BOG's confidentiality and privacy regulatory requirements as well as relevant data protection laws (data security);

f. the service provider's business continuity and contingency measures, including recovery testing, for ensuring the continuation of the outsourced function in the event of problems and events that may affect the service provider's operations such as a systems breakdown, natural disasters, an inability of a significant subcontractor to provide services relevant to the outsourced function, and situations where extraordinary demands are placed on a service provider;

g. reliance on and success in dealing with subcontractors;

h. adequacy of insurance coverage;

i. business objective, human resource policies, service philosophies, business culture and how they fit with those of the RFI;

j. external environment such as political, economic, social, legal, and regulatory environment of the jurisdiction in which the service provider operates from;

k. ability of the service provider to appropriately protect the confidentiality, integrity, and availability of data and of the systems and processes that are used to process, transfer or store those data[5] ; and

l. possibility of risk arising from concentration in the provision of some outsourcing services to RFI level of service provider's operational resilience to safeguard the RFI's critical operations in both normal circumstances and in the event of disruption.

47. An RFI shall conduct periodic (at least biannually) due diligence on existing service providers that have a contract term of more than two (2) years.

48. An RFI shall ensure that the outcomes of the due diligence process are well-documented and escalated to the Board, where relevant, in line with its outsourcing risk management framework.

Minimal Contractual Requirements with Service Providers

49. The BOG requires all outsourcing arrangements to be governed by written contract/agreement that clearly addresses all material elements of the arrangement including rights, responsibilities, and expectations of all parties (including the service provider and its sub-contractors), and the legality and enforceability of such contracts should be assessed by the RFI's legal counsel.

50. RFIs shall address all issues relevant to managing the risks associated with each outsourcing arrangement to the extent feasible and reasonable given the circumstances and having regard to the interests of the RFI.

51. Intra-group outsourcing arrangements shall be governed by an outsourcing agreement that meets the requirements set out in this Directive.

52. Minimum contractual requirements with service providers shall include among others:

a. nature and scope of the activities, functions or services being provided;
b. duration of the arrangement with date of commencement, expiry or renewal date and the notice period for the service provider and the RFI;
c. service levels and performance requirements;
d. operational, internal control, and risk management standards;
e. approval rights;

[5] An RFI should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements.

f. reporting requirements[6];
g. resolution of differences, defaults and termination;
h. indemnification and limits on liability;
i. ownership and access including provisions that ensure that the data owned by RFI can be accessed in the case of insolvency, resolution, or discontinuation of business operations of the service provider;
j. business contingency planning;
k. audit rights and access to records by the RFI and the BOG, and obligation of the service provider to cooperate with the BOG;
l. subcontracting, confidentiality, security, and separation of property including adherence to the Bank of Ghana's Cyber and Information Security Directive (CISD);
m. clauses that set out rules and limitations on sub-contracting and makes the service provider contractually liable for the performance and risk management practices of its sub-contractor and for the sub-contractor's compliance with the provisions in its agreement with service provider, including adherence to all provisions of this Directive;
n. complaints management and escalation procedures, pricing, insurance, and compliance;
o. termination clause in accordance with applicable laws, and minimum periods to execute a termination provision, where necessary[7];
p. conditions of subcontracting by the service provider, where appropriate; and
q. applicable laws and regulations.

53. Any outsourcing agreement shall not affect the rights of customers towards the RFI, including their ability to obtain redress.

54. RFIs shall ensure that written agreements especially those relating to outsourcing of core functions give the RFI and BOG all the necessary rights to ensure that the service provider and its sub-contractor are delivering on the relevant functions in line with applicable legal and regulatory requirements, and contractually agreed performance and risk indicators.

55. RFIs shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, the service provider shall be legally obliged to cooperate fully with both the RFI and new service provider (s) to ensure there is a smooth transition. In addition, the agreement shall ensure that the service provider is prohibited from erasing, purging, revoking,

[6] This includes, where applicable, the requirement for service providers to inform the RFI of any breach of security or confidentiality of outsourced data and obligations to submit reports of the internal audit function of the service provider.
[7] Such clause should include provisions relating to insolvency or other material changes in the corporate form, and clear delineation of ownership of intellectual property following termination, including transfers of information back to RFI.

altering or changing any data during the transition period, unless specifically advised by the BOG/ concerned RFI.

56. RFIs shall ensure that their contractual agreements with outsourcing service providers do not impair their ability to meet regulatory obligations. This includes the requirement to ensure that the contractual agreements grant RFIs and BOG rights to access, audit and obtain information (including access to all security information and logs of interest to the BOG in line with the CISD) from the service provider.

57. To facilitate the transfer of the outsourced functions to another service provider, the written outsourcing arrangement shall:

    a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the RFI, including the handling of data;
    b. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and
    c. include an obligation of the service provider to support the RFI in the orderly transfer of the function in the event of the termination of the outsourcing agreement.

58. In the case of cloud or other ICT outsourcing, RFIs shall define data and system security requirements within the outsourcing agreement.

Monitoring and Control of Outsourcing Arrangements

59. RFIs shall establish a structure, which includes effective procedures for monitoring the performance of, and managing the relationship with, the service provider (including its sub-contractors) and the risks associated with the outsourcing arrangements.

60. An RFI shall put in place, at a minimum, the following measures for effective monitoring and control of any outsourcing arrangement:

    a. A register of all outsourcing arrangements and ensure that the register is readily accessible for review by the Board and Senior Management of the RFI. The register shall be updated promptly and form part of the oversight and governance reviews undertaken by the Board and Senior Management of the RFI;

    b. Establish multi-disciplinary outsourcing management groups with members from different risk and internal control functions including legal, compliance and finance, to ensure that all relevant technical issues and legal and regulatory requirements are met;

c. Establish outsourcing management control groups (staff with appropriate expertise) to monitor and control the outsourced function and its contract performance on an ongoing basis;

d. Periodic reviews, at least on an annual basis, on all material outsourcing arrangements including the service provider's financial condition and risk profile;

e. Develop and maintain reporting policies and procedures which can promptly escalate problems relating to the outsourced function to the attention of the Board and Senior Management of the RFI and their service providers;

f. Conduct comprehensive pre- and post- implementation reviews of new outsourcing arrangements or when amendments are made to the outsourcing arrangements; and

g. The monitoring and control procedures over the outsourcing arrangement shall be subject to regular reviews by the internal audit.

Data Protection and Confidentiality

61. An RFI shall ensure that appropriate controls are in place and are effective in safeguarding the security, confidentiality, availability and integrity of any information shared with the service provider. In meeting this requirement, an RFI shall ensure that:

    a. information disclosed to the service provider is limited to the extent necessary to provide the contracted service, and only on a need-to-know basis;

    b. information shared with the service provider is used only to the extent necessary to perform the obligations under the outsourcing agreement;

    c. all locations (in country/offshore) where information is processed or stored, including back-up locations, are made known to the RFI;

    d. where a service provider is located, or performs the outsourced function, outside Ghana, the service provider is subject to data protection standards that are comparable to Ghana and must not impede effective supervision or hinder the business operations of the RFI;

    e. adequate controls in place to ensure that the requirements of customer data confidentiality are observed, and proper safeguards

are established to protect the integrity and confidentiality of customer information; and

f. no outsourcing arrangements may result in the disclosure of customer information to third parties without the prior consent of the customer.

Anti-Money Laundering Requirements

62. RFIs shall demonstrate to the BOG that under the outsourcing arrangement, statutory requirements on Anti-Money Laundering/CFT in Ghana as well as record keeping procedures and practices will continue to be met at all times.

Environmental, Social and Governance (ESG) Requirements

63. When selecting service providers, RFIs shall carefully pay attention to human rights and consider the impact of their outsourcing on all stakeholders; this includes taking into account their social and environmental responsibilities and adhering to all regulations surrounding ESG. Such aspects are of particular relevance when service providers are located offshore.

Audit and Inspection

64. In all its agreements for material outsourcing arrangements, an RFI shall include clauses that:

a. allow the RFI to conduct audits on the service provider and its sub-contractors, either directly or through its agents, and to obtain any report or findings on the outsourcing arrangements from the service provider and its sub-contractors; and

b. grants BOG and its agents the contractual rights to access and inspect the service provider and its subcontractors, and to obtain relevant records and documents pertaining to the RFI's transactions and information that is stored at or processed by the service provider and its subcontractors[8].

65. Following a risk-based approach, the Internal Audit Function (IAF) of the RFI shall undertake independent reviews of all outsourced activities.

[8] These include the reports and documents produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to the outsourcing arrangement.

Specifically, as part of its engagement, IAF shall assess the following in relation to outsourcing process:

a. whether the RFI's outsourcing policies are effectively implemented and are in line with the applicable laws and regulations and the RFI's risk strategy;

b. the adequacy, quality, and effectiveness of the materiality and risk assessment of outsourced functions;

c. quality of Board and senior management oversight of outsourcing arrangements; and

d. quality of monitoring and management of outsourcing arrangements.

Intra-group Outsourcing Arrangements

66. Where an RFI intends to outsource a function to entities within the same group, the selection of a group entity shall be based on objective reasons and conditions of the outsourcing arrangement and are set at arm's length and include safeguards to deal with conflicts of interest issues associated with the outsourcing arrangement.

67. RFIs shall clearly identify all relevant risks and detail the mitigation measures and controls put in place to ensure that the outsourcing arrangements with affiliated entities do not impair the RFIs' ability to comply with the relevant regulatory framework.

68. An RFI shall comply with its outsourcing risk management framework, as well as all requirements within this Directive in the intra-group outsourcing arrangement.

69. As appropriate, an RFI may undertake its outsourcing risk assessment making use of parent company analysis, risk management frameworks so long as the risk assessment is specific to the needs of the RFI's outsourcing arrangements and takes into consideration local legal and regulatory requirements.

70. The BOG may have additional requirements for a foreign parent/group arrangement, depending on the risks related to the outsourcing arrangement and the relevant findings from the BOG's supervisory review.

71. The contractual arrangement should grant RFI as well as the BOG rights to full access to all the records of the intra-group service provider and the rights to audit or undertake examinations of the service provider where appropriate either directly or through an appointed agent.

72. A service provider operating outside of Ghana shall comply with the relevant laws and regulations in Ghana including adhering to the data protection and cyber and information security laws of Ghana.

73. Where functions are provided by a service provider that is part of a group that is owned by the RFI or institutions that are members of a group, the conditions, including financial conditions for outsourced services should be set at arm's length.

74. The BOG may consult with regulators of a parent entity or relevant affiliate(s) to facilitate common understanding of group-wide risks and peculiar risks to the RFI.

Off-shore Outsourcing Arrangements

75. Where the outsourcing arrangement of an RFI's core function results in services being provided in or from a foreign jurisdiction, the RFI's risk management framework shall be enhanced to address any additional risk factors linked to the economic and political environment, social conditions, and events that could reduce the foreign service provider's ability to effectively provide the service on an ongoing basis.

76. An RFI shall pay particular attention to the legal requirements of the foreign jurisdiction relative to the minimum Ghanaian legal requirements and ensure that any gaps in requirements are addressed in the contract for the outsourcing arrangement.

77. An RFI as well as the BOG shall have full access to all data records of the service provider as well as any data or records of any subcontracting arrangements with foreign service providers.

78. RFIs shall not outsource to a jurisdiction which is inadequately regulated or which has secrecy laws that may hamper access to data by the BOG or RFIs' external auditors.

79. RFIs shall ensure that all outsourcing arrangements that fall under a technology transfer agreement are registered with the Ghana Investment Promotion Centre (GIPC) and shall comply with the GIPC Act, 2013 (Act 865) and The Technology Transfer Regulations, 1992 (L.I. 1547).

PART III – INFORMATION TECHNOLOGY FUNCTIONS

80. RFIs shall comply with all provisions of this Directive as well as the BOG's Cyber and Information Security Directive, 2018 and other relevant regulations with respect to outsourcing of Information Technology (IT) functions.

81. Outsourcing of IT functions shall include outsourcing of the following IT functions:

    a. IT infrastructure management, maintenance and support (hardware, software or firmware);

    b. Network and security solutions, maintenance (hardware, software or firmware);

    c. Application development, maintenance and testing; application service providers (ASPs) including ATM Switch ASPs;

    d. Services and operations related to Data Centres;

    e. Cloud computing services;

    f. Managed security services; and

    g. Management of IT infrastructure and technology services associated with payment system ecosystem.

82. RFIs shall ensure that their Security Information and Event Management (SIEM) system shall be connected to all outsourced IT functions, which shall be connected to the BOG's SIEM and in compliance with all relevant requirements in the BOG's Cyber and Information Security Directive, 2018.

83. IT functions that would not be considered as outsourcing arrangements of IT functions are noted in Annexure IV.

84. Additional requirements pertaining to usage of cloud computing services and outsourcing of Security Operations Centre (SOC) services, other than the provisions in the BOG's Cyber and Information Security Directive, 2018, are outlined in Annexure VI and VII, respectively.

PART IV – APPROVAL REQUIREMENTS FOR MATERIAL OUTSOURCING ARRANGEMENTS

Application Process and Overall Timing

85. An RFI shall submit to the BOG an application to outsource a core function.

86. The application shall include the information requirements outlined in this Directive.

87. The BOG shall acknowledge receipt of such application in writing within ten (10) working days of receipt of the application. The letter of acknowledgement shall indicate whether there are deficiencies in the submitted application/ information.

88. The BOG may arrange to meet with the representatives of the RFI requesting approval in order to address any issues which may require further clarification.

89. The BOG reserves the right to request additional information not listed in this Directive if considered relevant to the application for approval of the material outsourcing arrangement.

90. Once satisfied, in accordance with Section 60 (12) of Act 930 or Section 57 (12) of Act 1032, the Bank of Ghana shall issue an approval in writing to the RFI to outsource the core function or activity.

91. If a material outsourcing arrangement is renewed or amended, including assignments to third parties, the RFI shall apply to the BOG for re-assessment and approval.

Information Requirements

92. RFIs seeking approval of a material outsourcing arrangement shall submit to the BOG as part of the application, the following minimum information requirements:

    a. covering letter requesting approval in accordance with Section 60 (12) of Act 930 or Section 57 (12) of Act 1032 outlining the type of core function to be outsourced and an explanation as to why this is considered a core function;

    b. draft copy of the outsourcing agreement/contract with an explanation, if any, of non-compliance with the minimum contractual requirements as provided in this Directive;

c. copy of the RFIs' outsourcing risk management framework, including the policies and procedures pertaining to the management of material outsourcing arrangements;

d. results of the RFIs' materiality and due diligence assessments;

e. name and credentials of the principal contact at the RFI that will oversee the management and monitoring of the outsourcing arrangement;

f. copy of the risk register of all outsourcing arrangements currently in force/place at the RFI;

g. where the proposed outsourcing arrangement is with a foreign service provider, evidence that the service provider is aware and will adhere to Ghanaian laws, regulations, directives specifically with respect to the BOG's powers relating to access of records, examination/investigation rights;

h. where the proposed outsourcing is an intra-group outsourcing arrangement, an explanation as to the nature of the relationship within the financial holding company or financial group. If the intra-group service provider is regulated in a foreign jurisdiction, the name of the regulatory agency as well as the contact information at the foreign regulatory authority;

i. attestation from the proposed service provider acknowledging the BOG's requirements pertaining to customer and confidential information and data security; and

j. evidence of compliance with the technology transfer legislation, if applicable.

93. RFIs shall submit through the BOG's online reporting system, the above information requirements and any other particulars that the BOG may require.

PART V – SANCTIONS AND REMEDIAL MEASURES

94. An RFI that fails to comply with the requirements of this Directive shall be liable to pay to the Bank of Ghana an administrative penalty of one thousand penalty units (as per section 60 (13) of Act 930 or section 57 (13) of Act 1032) as well as applicable remedial measures and related sanctions as set out in Act 930 or Act 1032.

PART VI – REGULATORY REPORTING AND DISCLOSURE REQUIREMENTS

95. RFIs shall submit to BOG all internal audit reports on core outsourcing functions.

96. RFIs are required to inform BOG in a timely manner of any material changes or severe events, including cyber incidents, affecting their outsourcing arrangements and which could have a material impact on the continuing provision of the RFIs' business activities. This includes any event that could potentially lead to prolonged service failure or disruption or any breach of security and confidentiality of customer information.

97. An RFI shall notify BOG if any foreign supervisory authority or agency were to seek access to its customer information or if a situation were to arise where the rights to access the service provider by the RFI and BOG were to be restricted or denied.

98. An RFI shall disclose in its Audited Financial Statements an aggregate list of all existing core and non-core outsourced functions and service providers (including sub-contractors) as at the end of the reporting year.

ANNEXURES
ANNEXURE I – EXAMPLES OF CORE AND NON-CORE FUNCTIONS

1. Examples of ***core functions*** which an RFI may outsource to a service provider requiring the prior approval of the Bank of Ghana (Non-Strategic Function) include, but are not limited to:

    a. cyber and ICT systems (major hardware/software), management and maintenance (e.g. software development, data entry and processing, data centres, facilities management, end-user support, local area networks, web-site hosting and development, internet accessing and help desk);
    b. disaster recovery site;
    c. document processing (e.g. cheques, credit card slips, bill payments, bank statements, other corporate payments);
    d. processes (application processing like loan originations, collateral management, loan administration which includes debt collection -);
    e. portfolio management (e.g. investment advice, portfolio and cash management);
    f. marketing and research (e.g. product development, data warehousing and mining, advertising, media relations, call centres, telemarketing);
    g. back-office management (e.g. electronic funds transfer, payroll processing, custody operations, quality control, purchasing);
    h. real estate administration (e.g. building maintenance, lease negotiation, property evaluation, rent collection);
    i. professional services related to the business activities of the RFI (e.g. accounting, legal and actuarial etc); and
    j. human resources (e.g. benefits, administration, recruiting and training for capacity building).

2. Examples of ***non-core functions*** which an RFI may outsource to a service provider without the prior approval of the Bank of Ghana include, but not limited to:

    a. courier services, regular mail, utilities, telephone;
    b. procurement of specialised training;
    c. discrete advisory services (e.g. certain investment advisory services that do not result directly in investment decisions, etc);
    d. purchase of goods, wares, commercially available software and other commodities;
    e. printing services;
    f. repair and maintenance of fixed assets;
    g. supply and service of leased telecommunication equipment;
    h. travel agency and transportation services;
    i. maintenance and support of licensed software;
    j. temporary help and contract personnel;

k. fleet leasing services;
l. catering services;
m. cleaning services;
n. specialised recruitment; and
o. external conferences.

3. RFIs are required to notify the Bank of Ghana, in writing, of its intention to outsource **non-core functions** ten (10) days prior to engaging the service provider.

4. An RFI shall request in writing to the BOG to determine whether a function to be outsourced is a core or non-core function and/or a strategic or non-strategic function, where that function is not listed in this Directive.

ANNEXURE II – EXAMPLES OF CORE FUNCTIONS WHICH SHALL NOT BE OUTSOURCED (STRATEGIC FUNCTIONS)

1. Examples of core functions which an RFI shall not outsource to a service provider (strategic functions) include, but not limited to:

    a. Board and Senior Management functions such as strategic oversight, corporate planning, organization, management and control and decision-making functions;
    b. decisions on whether or not to grant credit;
    c. determining compliance with Anti-Money Laundering and Combating of Financing of Terrorism and Know Your Customer (KYC) norms for opening accounts;
    d. internal audit function;
    e. risk management function;
    f. compliance function;
    g. treasury function; and
    h. financial control

2. An RFI may apply to the BOG for an exemption to outsource a strategic function based on certain factors such as size and complexity of the RFI or intra-group outsourcing arrangement. Such applications shall be reviewed by the BOG on a case-by-case basis.

ANNEXURE III – SAMPLE QUESTIONS TO ASSESS THE MATERIALITY OF OUTSOURCING ARRANGEMENTS

1. In assessing the materiality of a specific outsourcing arrangement, an RFI shall consider the following questions, among others:

    a. What is the relationship between the business activity and the RFI's core business?
    b. What is the impact of that function to be outsourced on the RFI's earnings, solvency, funding, capital and reputation?
    c. What is the outsourcing arrangement's potential impact on earnings, solvency, liquidity, funding, capital, reputation, internal expertise and capacity of the RFI, ability to meet customer's obligations, brand value or system of internal controls?
    d. What is the outsourcing arrangement's potential impact on customer or confidential information or on data security and the overall risk profile of the RFI?
    e. What is the outsourcing arrangement's importance to achieving and implementing the business objectives, business strategy and business model?
    f. What is the RFI's aggregate exposure to a particular service provider? Is the RFI exposed to additional outsourcing risk as a result of multiple outsourcing arrangements with a service provider?
    g. What is the size of contractual expenditures as a share of non-interest expenses of the RFI or line of business?

2. If the service provider is unable to perform the service over a given period of time:
    a. What is the expected impact on the RFI's customers?
    b. What is the likely impact on the RFI's reputation?
    c. Would it have a material impact on the RFI's risk profile?
    d. Would the RFI be able to engage an alternative service provider? How long would it take and what costs would be involved?

ANNEXURE IV – EXAMPLES OF FUNCTIONS WHICH SHALL NOT BE CONSIDERED AS OUTSOURCING ARRANGEMENTS

1. Examples of functions which would not be considered as outsourcing arrangements under this Directive include, but not limited to:

   a) correspondent banking services;
   b) market information services such as Bloomberg, Moody's, Fitch Ratings, Standard & Poor's;
   c) credit background investigation services such as Credit Reference Bureaus, Credit Rating Agencies;
   d) provision of collateral information services such as Collateral Registry, Central Securities Depository;
   e) common network infrastructures such as Visa and MasterCard;
   f) clearing and settlement arrangements between clearing and settlement institutions and their members and similar arrangements between members and non-members;
   g) independent audit/governance/tax reviews;
   h) director's certification training programme (paragraph 12c of the Corporate Governance Directive);
   i) independent consulting;
   j) global financial messaging infrastructure which are subject to oversight by relevant regulators (e.g. SWIFT)
   k) services the RFI is not legally able to provide; and
   l) one-time services offered by a third-party to an RFI.

2. Examples of IT functions which would not be considered as outsourcing arrangements under this Directive include, but not limited to:

   a) corporate Internet Banking services obtained by RFIs as corporate customers/ sub members of another RFIs;
   b) external audit such as Vulnerability Assessment/ Penetration Testing (VA/PT), Information Systems Audit, security review;
   c) SMS gateways (Bulk SMS service providers);
   d) procurement of IT hardware/ appliances;
   e) acquisition of IT software/ product/ application (like CBS, database, security solutions, etc.,) on a licence or subscription basis and any enhancements made to such licensed third-party application by its vendor (as upgrades) or on specific change request made by the RFI;
   f) any maintenance service (including security patches, bug fixes) for IT Infra or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the RFI;

g) applications provided by financial sector regulators or institutions like GhIPSS, GSE, etc.;
h) platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.;
i) any other off the shelf products (like anti-virus software, email solution, etc.,) subscribed to by the RFI wherein only a license is procured with no/ minimal customisation;
j) services obtained by an RFI as a sub-member of a Centralised Payment Systems (CPS) from another RFI;
k) market information services such as Bloomberg, Moody's, Fitch Ratings, Standard & Poor's;

ANNEXURE V – RISK REGISTER

1. RFIs shall maintain an updated register of information on all outsourcing arrangements and shall document all outsourcing arrangements distinguishing between core and non-core outsourcing arrangements. They shall also maintain the documentation of closed/ terminated outsourcing arrangements as part of the register and supporting documentation for an appropriate period taking into account the relevant legislation and regulatory requirements.

2. The register shall include at least the following information for **all** existing outsourcing arrangements:

    a. reference number for each outsourcing arrangement;
    b. the start date and, as where applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for RFI;
    c. a brief description of the outsourced function, including the data that are outsourced;
    d. a category reflecting the nature of the function outsourced to facilitate identification of different types of arrangements, e.g., information technology (IT), risk management control function;
    e. the name of the service provider, the corporate registration number, registered address (location) and other relevant contact details, and the name of its parent company (if any);
    f. the country or countries where the service is to be performed including where the data will be located (i.e. country or region);
    g. whether or not (yes/no) the outsourced function is considered core (critical or material), including, where applicable, a brief summary of the reasons why the outsourced function is considered critical or material;
    h. in the case of outsourcing to a cloud service provider, the cloud service and deployment models (e.g., public, private, hybrid, community etc), and the specific nature of the data to be held and the locations where such data will be stored;
    i. the date of the most recent assessment of the materiality of the outsourced function.

3. For the outsourcing of core functions, the register shall include at least the following additional information:

    a. RFIs and other firms within the scope of the prudential consolidation that also make use of outsourcing from the same service provider;
    b. whether the service provider or sub-contractor is owned by an RFI within the group or other members of the group or an insider to the RFI;

c. the date of the most recent risk assessment and a summary of the key findings;
d. the individual or decision-making body in the RFI that approved the outsourcing arrangement;
e. the governing law of the outsourcing agreement;
f. the dates of the most recent and next scheduled audits, where applicable;
g. where applicable, the names of any sub-contractors to which material parts of a core function are sub-outsourced, including the country where the sub-contractors are registered, where the service will be performed and, if applicable, the location where the data will be stored;
h. outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a core function into RFI or the impact of discontinuing the core function;
i. identification of alternative service providers in line with point (h);
j. whether the outsourced core function supports business operations that are time-critical;
k. the estimated annual budget cost; and
l. public IP addresses and domains.

4. The register for all outsourcing arrangements shall be submitted to the BOG in the template indicated in Annexure VIII.

ANNEXURE VI – USAGE OF CLOUD COMPUTING SERVICES

1. There are several cloud deployment and service models that have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity. Each of these models[9] come with corresponding service, business benefit and risk profiles.

2. In addition to the outsourcing requirements prescribed in this Directive, RFIs shall adopt the following requirements for storage, computing and movement of data in cloud environments:

   a. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs10. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.

   b. In engaging cloud services, RFIs shall ensure, inter alia, that its outsourcing policy addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The RFIs shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.

   c. In the adoption of cloud services, RFIs shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attendant risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the RFI and the Cloud Service Provider (CSP). RFIs

[9] For example, some cloud service and deployment models are: a) Infrastructure as a Service (IaaS): The service provides compute, storage, network, and other basic resources so that the client can develop and deploy their applications. b) Platform as a Service (PaaS): The service provides software for building application, middleware, database, development environment and other tools along with the infrastructure to the client. c) Software as a Service (SaaS): Client uses the application(s) provided by the service provider on a cloud infrastructure. d) Besides application services, Cloud Service Providers (CSPs) also provide a range of services besides the three common services viz. Database as a Service, Security as a Service, Storage as a Service and others with varying risk levels. Deployment Models: cloud services are delivered through the popular models such as Private Cloud, Public Cloud, Hybrid Cloud, Community Cloud.

[10] For example, different heads of cloud related expenses could be application refactoring, integration, consulting, migration, projected recurring expenditure depending on the workloads, etc.

may refer to some of the *cloud security requirements and best practices*[11], for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services.

d. **Cloud Governance:** RFIs shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, *inter alia*, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.

e. **Considerations for selection of Cloud Service Providers (CSP)**: RFIs shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. RFIs shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to RFIs, including those relating to aspects such as data storage, data protection and confidentiality.

f. **Cloud Services Management and Security Considerations**

i. **Service and Technology Architecture:** RFIs shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. RFIs shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the RFI. The architecture should provide for a standard set of tools and processes to manage containers, images, and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks, and against co-mingling of data. The architecture should be resilient and enable smooth recovery in case of failure of any one or combination of components across the cloud architecture with minimal impact on data/ information security.

ii. **Identity and Access Management (IAM):** IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an

[11] BOG's Cyber and Information Security Directive, Cybersecurity Act, 2020 (Act 1038), and other international standards such as National Institute of Standards (NIST) and ISO 27001.

on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges'. In addition, multi-factor authentication should be implemented for access to cloud applications.

iii. **Security Controls:** RFIs shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the RFI; necessary procedures to authorise changes to cloud applications and related resources.

iv. **Robust Monitoring and Surveillance:** RFIs shall accurately define minimum monitoring policy requirements and procedures in the cloud environment. RFIs should ensure to assess the information/ cyber security capability of the cloud service provider, such that, the:

- CSP maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats;
- CSP is able to maintain its information/ cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment;
- nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the RFI and the threat environment; and
- CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, where applicable.

v. Appropriate integration of logs, events from the CSP into the RFI's SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud.

vi. The RFI's own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / RFI shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.

vii. Vulnerability Management: RFIs shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.

g. **Disaster Recovery & Cyber Resilience**

i. The RFI's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the RFI can continue its critical operations with minimal disruption of services while ensuring integrity and security.

ii. RFIs shall ensure that the CSP puts in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them. This should be systematically ensured, *inter alia*, through robust incident response and recovery practices including conduct of Disaster Recovery (DR) drills at various levels of cloud services including necessary stakeholders.

h. The following points may be evaluated while developing an exit strategy:

i. the exit strategy and service level stipulations in the SLA shall factor in, inter alia:
   - agreed processes and turnaround times for returning the RFI's service collaterals and data held by the CSP;
   - data completeness and portability;
   - secure purge of RFI's information from the CSP's environment;
   - smooth transition of services; and
   - unambiguous definition of liabilities, damages, penalties and indemnities.

ii. monitoring the ongoing design of applications and service delivery technology stack that the exit plans should align with.

iii. contractually agreed exit / termination plans should specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the RFI's business, while maintaining integrity and security.

iv. All records of transactions, customer and operational information, configuration data should be promptly taken over in a systematic manner from the CSP and purged at the CSP-end and independent assurance sought before signing off from the CSP.

i. **Audit and Assurance:** The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, inter alia, aspects such as roles and responsibilities of both RFI and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response, and resilience preparedness and testing, etc.

ANNEXURE VII – OUTSOURCING OF SECURITY OPERATIONS CENTRE

1. Outsourcing of Security Operations Centre (SOC) operations has the risk of data being stored and processed at an external location and managed by a service provider or sub-contractor (Managed Security Service Provider (MSSP)) to which RFIs have lesser visibility. To mitigate the risks, in addition to the controls prescribed in this Directive, RFIs shall adopt the following requirements in the case of outsourcing of SOC operations:

    a. unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);

    b. ensure that the RFI has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the RFI);

    c. assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;

    d. integrate the outsourced SOC reporting and escalation process with the RFI's incident response process; and

    e. review the process of handling of the alerts / events.

ANNEXURE VIII – OUTSOURCING RISK REGISTER TEMPLATE

OUTSOURCING RISK REGISTER TEMPLATE											
S/N	Name of Service Provider and its Sub-Contractor	Name of Service Provider's Parent Company	Outsourced Service	Indicate whether service is material to the RFI or its Group (Core or Non-Core)	Short description of Arrangement	Country from which Service is Provided	Applicable Laws Governing the Contract	Expiry/ Renewal Date of Contract or outsourcing Agreement	Estimated Annual Spending on Arrangement	Estimated GHS Value of Contract or Outsourcing Agreement	Other Remarks