BANK OF GHANA

OUTSOURCING DIRECTIVE

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

NOVEMBER 2024

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.

Per Principle 25 (Operational Risk and Operational Resilience) of the Basel Core Principles for Effective Supervision (BCP) issued by the Basel Committee for Banking Supervision (BCBS) in April 2024, supervisors are to require Board and Senior Management of RFIs to understand the risks associated with banking activities performed by Service Providers and ensure that effective risk management policies and processes are in place to adequately manage these risks.

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 shall be cited as the **Bank of Ghana Outsourcing Directive, 2024.**

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 Act 1032) 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 process, service, task or activity that is considered material (critical) 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, task 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 regulatory/legal 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 on a continuing basis 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 on a continuing basis that would otherwise be undertaken by the RFI itself;*

"Non-Outsourcing 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;*

"Related Interest" *in relation to an insider means*

a. *a firm or company in which an insider is interested, directly or indirectly as a director or controlling shareholder, partner, proprietor, employee or guarantor; and*
b. *a holding company, subsidiary, or affiliate of that company in which an insider is interested, directly or indirectly, as director, key management personnel, controlling shareholder, partner, proprietor, employee or guarantor;*

"Related Persons" *in relation to an insider means a spouse, son, daughter, step son, step daughter, brother, sister, father, mother, cousin, nephew, niece, aunt, uncle, step sister and step brother of an insider;*

"Security Information and Event Management (SIEM)" *means centralised logging software that can facilitate aggregation and consolidation of logs from multiple information system components, audit record correlation and analysis, correlation of audit record information with vulnerability scanning information in order to determining the veracity of the vulnerability scans and correlating attack detection events with scanning results*;

"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/ Third-party Service Provider (TPSP)" *means a natural or legal person (including third party as well as a parent bank or holding company and related entities within a group), domestic or foreign, that performs outsourced functions on behalf of an RFI. Such a person may be regulated or unregulated;*

"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 company secretary, legal, human resource, back-office management and other customer-related functions (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.*

Objectives

4. 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. Set BOG's supervisory approach to outsourcing;

   e. Ensure that material outsourcing arrangements with Service Providers and their sub-contractors do not pose excessive risk to RFIs; and

   f. 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 effectively managed to ensure that an RFI can meet its financial and service obligations to customers, and other stakeholders;

      iii. dealings between an RFI and outsourced Service Providers are conducted at arm's length.

Prior Approval Requirement

5. 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

6. 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

7. Regarding 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 relating to the outsourcing arrangement.

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. 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, relevant analysis together with a list of all immaterial (non-core functions) that the RFI has outsourced. The RFIs shall also make the aforementioned 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.

10. The BOG shall, in the course of its on-site examinations, off-site monitoring, or prudential dialogue with RFIs, establish whether outsourcing risks have been adequately assessed and addressed. The BOG shall review an RFI's implementation of this Directive, the quality of its Board and Senior

Management oversight, internal controls, and risk management regarding effectiveness of assessing and managing outsourcing risks to identify gaps for corrective action/supervisory intervention.

11. As part of its ongoing supervisory activities, the BOG shall assess the effectiveness of an 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.

12. BOG shall take into account outsourcing activities as an integral part of an on-going assessment of an RFI.

Transitional Arrangements and Effective Implementation

13. RFIs with existing outsourcing contracts/ arrangements in place that do not meet the requirements in this Directive shall:

    a. Review such contracts (including systems, processes as well as infrastructure) and ensure compliance with this Directive on the earlier of either the renewal date of the contract or by 30th June 2025; 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 VII; and
        ii. Material outsourcing contracts identified in (b)(i) above which do not comply with this Directive and indicate areas of non-compliance as well as a remedial plan, including a timeframe within which to address the weaknesses or deficiencies.

14. An RFI shall submit its materiality assessment framework to the BOG not later than 2nd June 2025.

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, in writing, within ten (10) working days prior to engaging the Service Provider.

16. New proposed outsourcing arrangements, including renewals, amendments and extensions of contracts or outsourcing agreements, with a Service Provider/ sub-contractor 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. However, where approval is required under any other BOG directives or guidelines, the RFI shall comply.

18. The effective implementation date of this Directive shall be **1st July 2025.**

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 to be performed "in house". RFIs 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. In this regard, the Board shall further ensure that the appropriate governance structures and processes are established for sound and prudent risk management;

    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 an 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. 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;

j. approving an exit strategy to enable an RFI 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. undertaking regular reviews and monitoring of the outsourcing arrangements and strategies for continued relevance, to support safety and soundness;

l. establishing a sound internal governance structure that provides effective oversight and control over outsourcing arrangements, which are consistent with the RFI's overall business strategy and risk appetite;

m. 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. In the case of an outsourcing to an affiliate, 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.

n. ensuring that the group-wide outsourcing risk management framework adequately addresses outsourcing risk across entities within the group, where an RFI (parent) has oversight responsibilities 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 an outsourcing arrangement, risk management framework, policies, procedures, monitoring tools, and metrics;

b. evaluating the materiality and risks from all existing and prospective outsourcing arrangements, based on the outsourcing risk management 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 (non-strategic) functions outsourced to a Service Provider;

j. ensuring that one internal unit, management committee or individual (key management personnel) is identified as being responsible for the documentation, management, monitoring and control of each outsourced function 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;

o. obtaining written approval from the BOG prior to outsourcing of any core function to a Service Provider and/ or sub-contractor;

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

m. developing a 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.

Risk Management

22. The Board and Senior Management of an RFI shall ensure that the proposed outsourcing arrangement has been subject to a comprehensive risk assessment (in respect of legal, operational, and reputational risks) and that all the risks identified have been adequately addressed before launch. Specifically, the risk assessment should cover, at a minimum, the following:

    a. the importance, materiality and criticality of the functions to be outsourced;

    b. reasons for the outsourcing (this includes cost and benefit analysis); and

    c. the impact on an RFI's risk profile (this include operational, legal and reputational) of the outsourcing.

23. Risks may change throughout the life cycle of the outsourcing arrangement and therefore RFIs shall perform risk assessments on an ongoing basis.

24. 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;

f. assessing a Service Provider and its sub-contractors' ability to employ a high standard of care in performing the outsourced function and meeting 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, if any, to the Service Provider, to manage concentration risk;

i. incident detection, response and reporting system as well as policies and procedures to detect activities that may impact on a Service Provider's information security (including data breaches, IT/ 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 reviewed annually by the Board of an RFI 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.

[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.

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

26. RFIs shall ensure that a Service Provider and sub-contractor, 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 related interest and related persons.

27. An RFI shall ensure that an outsourcing arrangement neither diminish its ability to fulfil its obligations to customers and regulators, nor impede effective supervision by the BOG**.**

28. 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.

Business Continuity Planning

29. RFIs shall develop, maintain and regularly test appropriate business continuity plans with regard to outsourced core functions[4]. Such plans shall take into account:

    a. the possible events that may lead to the quality of the provision of the outsourced core functions deteriorating to unacceptable levels or fails;

    b. the potential impact of insolvency or other failure of the Service Provider; and

[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).

c. political/ country risk in the Service Provider's jurisdiction, where relevant.

30. RFIs shall have a documented exit strategy when outsourcing core functions by migrating to another Service Provider or by reintegrating the core outsourced function, that is in line with their outsourcing policy and business continuity plans, and which should take into account at least the possibility of:

    a. termination of outsourcing arrangements;

    b. failure of the Service Provider;

    c. deterioration in the quality of the outsourced function; and

    d. material risks inherent in the outsourced function exceeding the outsourcing risk appetite of the RFI.

31. RFIs shall ensure that the agreement has necessary clauses on safe return and/ or safe removal/ destruction of data, hardware and all records (digital and physical), as applicable when the outsourcing arrangement is terminated. 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, altering or changing any data during the transition period, unless specifically advised by the BOG/ concerned RFI.

Data Protection and Confidentiality

32. RFIs shall take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, legal and regulatory compliance (including Data Protection Act, 2012 (Act 843), as well as auditing. RFIs should, in particular, ensure that the Service Provider has:

    a. the ability to clearly identify and segregate customer data; and

    b. robust access controls to protect customer information.

33. 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 solely for the purpose of performing 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 that of Ghana and should not impede effective supervision or hinder the business operations of the RFI;

e. adequate controls are put 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;

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

g. the level of security controls, governance, policies, and procedures at the Service Provider and sub-contractor are robust to protect the security and confidentiality of information shared under the outsourcing arrangement.

Materiality Assessment

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

35. 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.

36. The materiality assessment shall be undertaken prior to entering into any outsourcing arrangement in line with the RFI's approved materiality assessment framework, with the end result being a determination of whether the outsourcing arrangement is considered a core or non-core function.

37. 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 are provided in Annexure I. These are however not extensive.

38. 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. These are however not extensive.

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

    a. the impact of the outsourcing arrangement on earnings, solvency, liquidity, funding, capital, ability to meet customers' obligations, reputation and 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 long-term effects of failure by a Service Provider on an RFI's reputation;

    d. the effect of an outsourcing arrangement on an RFI's ability to meet regulatory and legal reporting requirements;

    e. the degree of difficulty and time required to find an alternative Service Provider or reintegrate the business activity in-house, where necessary;

    f. the potential that multiple outsourcing arrangements provided by the same Service Provider can have a significant impact – in aggregate – on the RFI;

    g. whether the Service Provider is given access to the RFI's general ledger or confidential customer information;

    h. whether an information security breach, other operational failure, or misconduct by the Service Provider or its employees and agents could

plausibly lead to the RFI's inability to operate a material business line for more than 48 hours, or if the failure would plausibly lead to public exposure of confidential customer information; and

i. impact on an RFI's customers, and counterparties should the Service Provider fail to perform the service or encounter a breach of confidentiality or security.

40. In establishing supervisory thresholds for materiality assessments (the quantitative limits shall be estimated based on the recent Audited Financial Statement), RFIS shall consider an outsourcing arrangement material if:

a. its annual payments to the Service Provider is 5% or more of its total operating cost[5];

b. 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;

c. the earnings 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);

d. 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); and

e. cost to bring the outsourced activity in-house or to seek similar service from another Service Provider due to failure of the Service Provider (a threshold of 5% or more as a proportion of total operating cost of the RFI).

41. Where an outsourcing arrangement with a Service Provider covers multiple functions, an RFI should consider all aspects of the arrangement with the materiality assessment.

42. An RFI shall undertake annual reviews of its outsourcing arrangements to identify new outsourcing risks as well as materiality. Results of this review may indicate that an outsourced function which was previously assessed as immaterial may subsequently become material due to incremental services from the Service Provider or change in nature of the outsourced service.

[5] Reference date to be considered in the initial materiality assessment shall be the contract awarding date. Subsequent annual materiality assessment shall adopt the date of implementation of the contract as reference date to be used in computing total operating cost.

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

Due Diligence Processes

44. In selecting a Service Provider or renewing an outsourcing arrangement, 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.

45. The due diligence shall 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 business strategy.

46. 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.

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

    a. experience, capacity, operational and technical competence of the Service Provider to implement and support the outsourced function. This may include the review of the experience and technical competence of significant subcontractors where feasible;

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

    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. effectiveness of internal controls, risk management, audit coverage, reporting and monitoring environment of the Service Provider;

    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, contingency measures and operational resilience, 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 sub-contractor to provide critical 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 sub-contractors;

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. assessment of relative costs and benefits associated with the outsourcing arrangement. RFIs shall consider at a minimum the following:

    i. the potential risks of not entering into an outsourcing arrangement against the risks that the new outsourcing arrangement may introduce or amplify known risks (e.g. replacing obsolete legacy system, difficulty in hiring and maintaining qualified staff);

    ii. the RFI's ability (including cost, timing, contractual restrictions) to exit the outsourcing arrangement and either transition to another Service Provider or bring the activity back in-house; and

    iii. the RFI's ability to adopt new and advanced technologies and the potential risks thereof.

l. the reputation of the Service Provider or sub-contractor in respect of services offered, the quality and dependability of its personnel;

m. ability of the Service Provider to appropriately protect the confidentiality, integrity, and availability of data as well as systems and processes used to process, transfer or store data[6] ; and

n. possibility of concentration risk emanating from reliance of RFIs on a common Service Provider and ability of the Service Provider to safeguard the RFI's critical services in both normal circumstances and in the event of disruption.

48. An RFI shall conduct due diligence annually on existing Service Providers that have a contract term of more than two (2) years.

49. An RFI shall ensure that the outcome of the due diligence process is well-documented and sent to the Board, where relevant, in line with its outsourcing risk management framework.

Minimum Contractual Requirements

50. All outsourcing arrangements shall be governed by clearly written and legally binding contract that clearly addresses all material elements of the arrangement. This shall include rights, responsibilities, and expectations of all parties (including the Service Provider and its sub-contractors), and the legality and enforceability of such contracts shall be assessed by the RFI's legal counsel.

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

52. Minimum contractual requirements governing outsourcing arrangements with Service Providers shall include:

a. nature and scope of the activities, including clear definitions of functions being provided;
b. duration of the arrangement/ agreement in respect of date of commencement, expiry or renewal date and the notice period for the Service Provider and the RFI to disengage/ amend the outsourcing agreement;
c. pricing and fee structure;
d. service levels and key performance benchmarks;
e. operational, internal control, and risk management expectations of the RFI with regards to the Service Provider;
f. approval rights with respect to amendments to the outsourcing agreement;

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

g. reporting requirements[7] for the Service Provider and sub-contractors;
h. resolution of differences and early exit clause in case of defaults by the Service Provider;
i. indemnification and limits on liability;
j. ownership and access including provisions that ensure that the data owned by RFI can be accessed in the case of insolvency, liquidation, receivership, change in ownership, or discontinuation of business operations of the Service Provider;
k. obligations and responsibilities relating to business continuity and disaster recovery planning (BCP/DRP) for services provided and to support the RFI's BCP and DRP testing as appropriate;
l. provisions on audit rights and access to records, which include the following:

    i. allows the RFI to conduct audits on the Service Provider and its sub-contractors, either directly or through its agents, and to obtain any accurate and timely report or findings on the outsourcing arrangements from the Service Provider and its sub-contractors; and

    ii. grants BOG and its agents the contractual rights to have direct, timely and unrestricted access to the systems of the Service Provider and any information or documents relating to the outsourced function as well as conduct on-site inspection of the Service Provider and sub-contractor[8], where necessary.

m. subcontracting, confidentiality, information security, resilience, and separation of property[9] including adherence to provisions of the BOG's Cyber and Information Security Directive (CISD);
n. clauses that set out rules and limitations on sub-contracting and makes the Service Provider responsible 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 the Service Provider which shall be in line with provisions of this Directive;
o. complaints management and escalation procedures, pricing, insurance, and compliance of the Service Provider;

[7] 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.
[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.

[9] Separation of property agreement should outline how assets and responsibilities are divided fairly during separation or termination of the outsourcing agreement.

p. termination clause in accordance with applicable laws, and minimum periods to execute a termination provision, where necessary[10]; and
q. adherence to applicable Ghanaian laws and regulations.

53. RFIs shall ensure that their contractual agreements with Service Providers do not impair their ability to comply with regulatory requirements.

54. To facilitate the transfer of the outsourced functions to another Service Provider, the written outsourcing agreement 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.

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

56. RFIs shall put in place Service Level Agreements (SLAs) with Service Providers and subcontractors with a combination of qualitative and quantitative targets.

Monitoring and Control of Outsourcing Arrangements

57. 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.

58. 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 regularly (quarterly), and form part of the oversight and governance reviews undertaken by the Board and Senior Management of the RFI;

[10] 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.

b. Establish multi-disciplinary outsourcing management control groups with members from different risk and internal control functions including legal, compliance and finance to:

   i. monitor and control the outsourced function and its contract performance on an ongoing basis; and
   ii. ensure that all relevant technical issues as well as legal and regulatory requirements are met.

c. Conduct regular reviews, annually, on all material outsourcing arrangements including the Service Provider's governance arrangement, financial condition, key performance benchmarks, and risk profile as well as impact of the outsourcing arrangement on the risk profile of the RFI;

d. Develop and maintain reporting framework (policy, processes 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;

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

f. The monitoring and control procedures over the outsourcing arrangement shall be subject to regular reviews by the internal audit function of an RFI.

Anti-Money Laundering Requirements

59. 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 shall continue to be met at all times.

Environmental, Social and Governance (ESG) Requirements

60. When selecting a Service Provider, an RFI shall carefully consider the impact of the RFI's outsourcing on all stakeholders; this includes taking into account RFI's social and environmental responsibilities and adhering to all regulations surrounding Environmental, Social and Governance (ESG) principles.

Audit and Inspection

61. Following a risk-based approach, the Internal Audit Function (IAF) of the RFI shall undertake independent reviews of all outsourced activities every two (2) years or less. Specifically, as part of its engagement, IAF shall assess the following in relation to the outsourcing arrangement:

    a. whether the RFI's outsourcing policies are effectively implemented and 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 control of outsourcing arrangements.

Intra-group Outsourcing Arrangements

62. 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. The arrangements shall be set at arm's length and include safeguards to deal with conflicts of interest issues associated with the outsourcing arrangement.

63. 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.

64. An RFI shall comply with its outsourcing Risk Management Framework, as well as all requirements within this Directive in the intra-group outsourcing arrangement.

65. As appropriate, an RFI may undertake its outsourcing risk assessment making use of its parent company's analysis and 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.

66. The outsourcing agreement shall grant the RFI as well as BOG, rights to fully access all records of the intra-group Service Provider relating to the outsourced function and the rights to audit or undertake examinations of the Service Provider where appropriate either directly or through an appointed agent.

67. 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.

68. Where functions are provided by a Service Provider that is part of a group owned by the RFI or institutions that are members of a group, the conditions, including financial obligations and conditions for outsourced services shall be set at arm's length.

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

70. The BOG may prescribe 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 reviews.

Off-shore Outsourcing Arrangements

71. 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 risks from 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.

72. 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 sub-contracting arrangements with foreign Service Providers relating to the outsourced function.

73. RFIs shall not outsource to a Service Provider in a jurisdiction which has secrecy laws that may hamper access to data by the BOG or RFIs' external auditors (i.e. impedes effective supervision and audit of the RFI).

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

PART III – INFORMATION TECHNOLOGY FUNCTIONS

75. 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)[11] functions.

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

    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. Security Information and Event Management (SIEM) services;

    g. Managed security services; and

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

77. RFIs shall ensure that their Security Information and Event Management (SIEM) system is 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.

78. Additional requirements pertaining to usage of cloud computing services, other than the provisions in the BOG's Cyber and Information Security Directive, 2018, are outlined in Annexure VI.

79. IT functions that are not considered as outsourcing arrangements of IT functions are noted in Annexure IV.

[11] Information Technology, within this Directive, includes information and cyber security as well as Technology.

PART IV – REGULATORY APPROVAL REQUIREMENTS FOR CORE FUNCTIONS (NON-STRATEGIC)

Application Process

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

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

82. 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 information submitted as per the application.

83. The BOG may arrange a meeting with representatives of the applicant RFI to address any issues which may require further clarification.

84. 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.

85. 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.

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

Information Requirements

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

    a. an application letter requesting approval in accordance with Section 60 (12) of Act 930 or Section 57 (12) of Act 1032 indicating the type of core function(s) to be outsourced and the reason(s) for outsourcing the function(s) as well as an explanation as to why this is considered a core function;

    b. a draft copy of the outsourcing agreement/contract;

c. a copy of the RFIs' outsourcing Risk Management Framework (RMF), 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 person at the RFI that will oversee the management and monitoring of the outsourcing arrangement;

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

g. where the proposed outsourcing arrangement is with an offshore 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 to records and inspection 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 as well as data security; and

j. evidence of compliance with the Technology Transfer Regulations, 1992 (L.I. 1547), where applicable.

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

PART V – SANCTIONS AND REMEDIAL MEASURES

89. 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 other relevant remedial measures and related sanctions as set out in Act 930 or Act 1032.

PART VI – REGULATORY REPORTING AND DISCLOSURE REQUIREMENTS

90. RFIs shall submit to BOG all internal audit reports on core outsourced functions in line with the provisions of this Directive, every two (2) years.

91. 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.

92. 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.

93. All outsourcing arrangements including non-core functions shall be included in the RFI's outsourcing risk register and the register submitted to BOG semi-annually.

94. Service Providers shall disclose to the RFI breaches in confidentiality with respect to customer information and the RFI shall immediately report to the BOG.

95. An RFI shall disclose in its Audited Financial Statements an aggregate list of all existing core and non-core outsourced functions, 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 and sub-contractor requiring the prior written 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, website hosting and development, internet accessing and help desk);
    b. external audit such as Vulnerability Assessment/ Penetration Testing (VA/PT), Information Systems Audit, security review;
    c. security information and event management (SIEM) services;
    d. some of the required functions for handling a security incident[12];
    e. legal function;
    f. company secretary;
    g. disaster recovery site hosting;
    h. registration of collaterals (landed property/ immovables) for loans and advances;
    i. document processing (e.g. cheques, credit card slips, bill payments, bank statements, other corporate payments);
    j. processes (application processing like loan originations, collateral management, loan administration which includes debt collection);
    k. portfolio management (e.g. investment advice, portfolio and cash management);
    l. marketing and research (e.g. product development, data warehousing and mining, advertising, media relations, telemarketing);
    m. call centre services and other customer-related media services;
    n. back-office management (e.g. electronic funds transfer, payroll processing, custody operations, quality control, purchasing);
    o. real estate administration (e.g. building maintenance, lease negotiation, property evaluation, rent collection);
    p. professional services related to the business activities of the RFI (e.g. accounting, legal and actuarial etc);
    q. cashier/ teller services;
    r. human resources (e.g. benefits, administration, recruiting and training for capacity building[13]); and
    s. and any other function as the BOG may determine.

[12] Refer to BOG's CISD.

[13] Training here refers to training services provided by the same service provider for more than one (1) financial year. This excludes the directors' certification training programme provided by BOG certified vendors in accordance with paragraph 12C of the Corporate Governance Directive.

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

   a. courier services, regular mail, utilities, telephone;
   b. procurement of specialised training;
   c. purchase of goods, wares, commercially available software and other commodities;
   d. printing services;
   e. repair and maintenance of fixed assets;
   f. travel/ transportation services;
   g. maintenance and support of licensed software;
   h. fleet leasing services;
   i. catering services;
   j. cleaning services;
   k. manned security services;
   l. external conferences; and
   m. and any other function as the BOG may determine.

3. RFIs shall notify the Bank of Ghana, in writing, of its intention to outsource **non-core functions** ten (10) working days prior to engaging the Service Provider.

4. An RFI shall request in writing (this shall include the materiality assessment of that function) 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 explicitly provided for in this Directive or the materiality assessment of the listed function indicates otherwise. For this purpose, the RFI shall provide a copy of the materiality assessment of that function to the BOG.

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 are 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. cyber and information security management function;
    g. security operations centre (SOC) – situation room;
    h. compliance function;
    i. treasury function; and
    j. financial control

2. An RFI, with the exception of banks, may apply to the BOG for an exemption to outsource a strategic function or aspects of the function based on the application of proportionality (certain factors such as size, risk profile 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) arrangements with payment card schemes 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); and
   k) 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) SMS gateways (Bulk SMS Service Providers);
   c) procurement of IT hardware/ appliances;
   d) 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;
   e) 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;
   f) applications provided by financial sector regulators or institutions (e.g. GhIPSS, GSE, etc.);
   g) platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.;

h) any other off-the-shelf products (e.g. anti-virus software, email solution, etc.,) subscribed to by the RFI wherein only a license is procured with no/ minimal customisation;
i) services obtained by an RFI as a sub-member of a Centralised Payment Systems (CPS) from another RFI; and
j) 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 where applicable, the 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 is 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), Taxpayer Identification Number (TIN)/ Ghana Card PIN 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 VII.

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[14] 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 costs[15]. 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, an RFI 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, (this includes 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

[14] 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.

[15] 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*[16], 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 shall, *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 shall provide for a standard set of tools and processes to manage containers, images, and releases. Multi-tenancy environments shall be protected against data integrity and confidentiality risks, and against co-mingling of data. The architecture shall 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 on-premise application, may be established for identity and

[16] 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.

access management to cloud-based applications. Segregation of duties and role conflict matrix shall 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 a 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.

3. The BOG prohibits the storage of customer information on public cloud as stipulated in paragraph 56(7) of the BOG's CISD

ANNEXURE VII – 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**	**TIN/ Ghana Card PIN**	**Indicate whether service is material to the RFI or its Group (Core or Non-Core)**	**Short description of Arrangement**	**Country/ City/ Region/ State 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**