CENTRAL BANK OF TRINIDAD & TOBAGO

GUIDELINE FOR THE MANAGEMENT OF OUTSOURCING RISKS

This Guideline sets out minimum standards for the management of Outsourcing Risks by regulated financial institutions.

February 2022

Table of Contents

1. INTRODUCTION

1.1 The Central Bank of Trinidad and Tobago ("Central Bank") has noted recent trends, which have shown that the use of third party service providers ("service providers") to carry out business activities and processes that the financial institutions themselves would normally undertake are increasing. Studies indicate that outsourcing in the financial services industry was initially limited to activities that did not pertain to the regulated financial institution's primary business, such as payroll and back office processing. More recently, however, commonly outsourced activities have included information technology, cloud computing, accounting, regulatory reporting, internal audit, electronic funds transfer, fintech product and services, investment management and human resources.

1.2 The Central Bank recognizes that financial institutions may have sound reasons to outsource certain functions. The main reasons put forward for outsourcing by entities generally are to reduce and control operating costs, achieve economies of scale, and to meet the challenges of technological innovation, increased specialization and heightened competition.

1.3 The outsourcing of business activities can however increase the financial institution's dependence on third parties, 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.

1.4 Outsourced services are also becoming increasingly complex and may increase an institution's exposure to strategic, reputational, compliance, operational, country, cyber and transaction risks[1]. Consequently, many regulators have issued guidelines to their regulated financial institutions to ensure that they effectively identify, monitor and manage the risks associated with outsourcing activities.

1.5 In light of the foregoing, the Central Bank must consider the impact of **material** outsourced activities, functions, and services when conducting a risk assessment of a regulated entity. The assessment will include *inter alia* a determination of whether the outsourcing arrangement hampers in any way the financial institution's ability to comply with its regulatory obligations.

1.6 Moreover, the Central Bank will consider the potential system risks posed where outsourced activities of multiple regulated entities are concentrated in a single or limited number of third party service providers.

[1] Explanations of the outsourcing risks are provided under Section 5.2 of this document.

2. PURPOSE, APPLICATION AND SCOPE

2.1 This Guideline for the Management of Outsourcing Risks sets out the expectations of the Central Bank for the management of risks arising from the outsourcing of **material** activities, functions, and services by its Regulated Financial Institutions (RFIs). The RFI is expected to consider the impact of outsourcing on the RFI and the financial group, as applicable, of all material outsourcing contracts including those put in place by local and foreign subsidiaries or parent companies.

2.2 The Guideline therefore establishes **minimum standards** for the management of outsourcing risks by RFIs. The principles detailed in this Guideline should be applied in accordance with the materiality of the risk posed by the outsourced activity or service. However, even where the activity or service is not material, RFIs should consider the appropriateness of applying the principles of this guideline in a manner proportionate to the risks posed by the outsourcing arrangement.

2.3 This Guideline also provides guidance on business activities, functions, processes or services that should not be outsourced.

2.4 Appendix 1 provides examples of some services that may be regarded as outsourcing for the purposes of this Guideline as well as services that are generally not intended to be subject to this Guideline. These are only examples and are not meant to be an exhaustive list. RFIs should consider the nature and materiality of outsourcing in applying the Guidelines.

3. DEFINITIONS

CBA	means the Central Bank Act, Chap. 79:02.
Cloud Computing	means a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage facilities, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
ECA	means the Exchange Control Act, Chap. 79:50.
FIA	means the Financial Institutions Act, Chap. 79:09.
Financial Group	has the meaning assigned to it in the FIA and IA.
IA	means the Insurance Act, 2018.

Intra-Group Outsourcing Arrangements	means the arrangement whereby a member of a financial group enters into a material outsourcing arrangement with another entity in the same financial group.
Material Outsourcing	means outsourcing of a business activity, function, process or service which, if disrupted, has the potential to significantly affect *inter alia* the financial institution's business operations, reputation or profitability.
Outsourcing[2]	means the regulated entity's use of a third party service provider (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity**.**
Regulated Financial Institution or (RFI)	means a financial institution that is regulated by the Central Bank and includes a financial institution either licensed or issued a financial holding company permit under the FIA; registered or issued a financial holding company permit under the IA; licensed under the ECA; and payment systems and/or payment services providers registered pursuant to the FIA or CBA.
Third party service provider /Service provider	means the provider of the outsourced activity, function or service that is not the RFI.

4. MATERIAL ACTIVITIES, FUNCTIONS OR SERVICES

4.1 The determination of materiality to the RFI of an outsourced activity, function, or service is important for proper risk identification, mitigation and management. The assessment of the materiality of an outsourcing arrangement is often subjective and depends on the circumstances faced by an individual RFI. Without limiting the scope of the materiality assessment, factors that the management of the RFI may use to determine whether an outsourcing contract is material may include:

4.1.1 the **impact on significant business lines** if the service provider should fail to perform over a given period of time and whether or not this would result in potential losses or issues to the RFI, its customers and their counterparts;

[2] Definition taken from pg. 4 of The Joint Forum's "Outsourcing in Financial Services", Basel Committee of Banking Supervision, February 2005.

4.1.2 the **level of contribution of the outsourced activity, function or service** to the RFI's income and profit, including the cost of the outsourcing arrangement as a proportion of its total operating costs;

4.1.3 the **ability of the RFI to maintain appropriate internal controls and meet regulatory requirements**, if the service providers were to experience financial, operational or other problems;

4.1.4 the **interrelationship of the outsourced activity, function or service with other activities, functions or services of the RFI**;

4.1.5 the **degree of difficulty and time that would be required to find an alternative service provider** or to establish the business activity in-house should this become necessary;

4.1.6 the **ability to control the risks** where more than one service provider collaborates to deliver an end-to-end outsourcing solution;

4.1.7 the **potential impact that a confidentiality breach or failure of data integrity** can have on the RFI and its customers;

4.1.8 the **potential legal and reputational risks** if the service provider fails to perform; or

4.1.9 the **aggregate exposure to a particular service provider** in cases where the RFI outsources various functions to the same service provider.

4.2 The RFI shall maintain a centralized list of all its outsourcing contracts, which should be updated on an on-going basis. The RFI should also identify the material outsourced services on the list using, *inter alia*, the factors specified in this section and submit only those services identified as being material to the Central Bank in the first instance in accordance with section 12.2.2 and thereafter, upon request.

4.3 All RFIs that outsource or intend to outsource functions, activities or services to a third party service provider shall establish a board approved Outsourcing Policy to guide the development and approval process for the outsourcing of material activities. The Outsourcing Policy must align with the principles set out in this Guideline.

4.4 The RFI must establish internal policies, procedures and systems to ensure adherence to the Outsourcing Policy. Such policies, procedures and systems must facilitate determination of the materiality of the outsourced activity. The results of the analysis should be well documented and be readily available for review by the RFI's internal audit function and the Central Bank. At a minimum, the following documentation should be made available upon request:

4.4.1 An attestation from the Senior Manager with responsibility for risk management that the requirements of sections 5.3 and 5.7 as well as Appendix 3 have been adequately addressed in the draft contract;

4.4.2 Details of the activity, service, or function(s) to be outsourced. In the case of cloud computing, details should also be provided with respect to the type of cloud service and deployment model i.e. public/private/hybrid/community cloud;

4.4.3 A copy of the due diligence conducted on the outsourced service provider (see section 5.4.2), including the key risks identified and how the risks will be mitigated; and

4.4.4 Details relating to the proposed service provider including the directors, key shareholders, as well as, whether or not the service provider will be accessing the services of a sub-contractor and the country where the service provider is registered or licensed.

5. OUTSOURCING PRINCIPLES

RFIs should be guided by certain principles to ensure effective corporate governance and risk management of outsourcing arrangements. The Central Bank has identified the following principles for the effective management of outsourcing risks by RFIs.

5.1 Principle 1 – Outsourcing Policy

The RFI must have in place a comprehensive outsourcing policy to guide the assessment of whether, and how, the RFI's activities, functions, processes and services can be appropriately outsourced. The Board of Directors must retain responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.

In particular, the RFI's **Board** should:

5.1.1 Approve the RFI's outsourcing policy and ensure that the RFI's outsourcing policy is in line with current regulatory and legislative requirements, its risk appetite, risk tolerance, and overall risk management strategy and framework;

5.1.2 Ensure that the RFI's risk management framework includes provisions to evaluate the risks and materiality of all existing and prospective outsourcing arrangements, as well as, the policies, procedures and systems that apply to such arrangements; and

5.1.3 Ensure that a process is implemented for the periodic review of the Outsourcing policy and approval of all material outsourcing contracts.

5.2. Principle 2 – Risk Management

The RFI's Senior Management should ensure that the outsourced activities and the relationship with the third party service provider are addressed in the RFI's established risk management framework.

Senior management should therefore:-

5.2.1 Develop and implement a sound outsourcing policy, which is commensurate with the nature, scope and complexity of the RFI's outsourcing arrangements. This policy should consider any regulatory requirements and must be approved by the RFI's Board;

5.2.2 Report to the Board on any significant issues or changes arising with regard to material outsourcing contracts or service providers;

5.2.3 Ensure that the RFI's risk management framework includes all associated risks and risk mitigation strategies of the RFI. Table 1 below, though not exhaustive, presents some of the specific risks associated with outsourcing that should be considered in developing the RFI's policy and risk management framework;

5.2.4 Be accountable for effective due diligence, oversight, and management of outsourcing relationships and responsible for all outsourcing decisions, except those that require board approval;

5.2.5 Ensure that management and employees within the lines of businesses who manage the service provider relationships have the relevant skills, as well as, distinct but interrelated responsibilities to ensure that material outsourcing contracts are managed effectively and commensurate with the RFI's level of risk and complexity;

5.2.6 Implement an effective process to manage risks related to service provider relationships in a manner consistent with the RFI's strategic goals, organizational objectives, risk appetite, risk management strategy and framework;

5.2.7 Maintain all ongoing outsourcing arrangements and relationships in accordance with the Board approved outsourcing policy;

5.2.8 Routinely review the effectiveness of the policy and amend the policy, where necessary, to ensure that it remains reflective of the RFI's risk appetite;

5.2.9 Ensure that adequate business continuity and contingency plans are in place in the event that the service provider is unable to fulfill the outsourcing contract;

5.2.10 Ensure that a risk evaluation is conducted to ensure that material outsourcing arrangements do not result in the internal controls, business conduct or reputation of the RFI being compromised or weakened. This evaluation should be performed at least annually on existing material outsourcing arrangements as part of the review processes of the RFI and be made available to the Central Bank upon request. As part of the risk evaluation, the RFI should:

a) identify and classify its activities, processes and related data and systems re: the sensitivity and required protections; and

b) define and decide on an appropriate level of protection for data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended outsourcing. With regard to cloud computing, RFIs should also consider specific measures where necessary for data in transit, data in memory, and data at rest, such as the use of encryption technologies in combination with appropriate key management architecture.

5.2.11 Ensure that key risks and risk mitigation strategies are identified, and the impact and potential benefits of the outsourcing arrangements are analyzed. For example, where outsourcing risks are higher such as, where the RFI outsources to an unregulated third party service provider, or to a service provider located in an overseas jurisdiction, the RFI must ensure that risk mitigation strategies are more robust (see Section 9 of this Guideline).

TABLE 1: Main Risks Inherent in Outsourcing

Inherent Outsourcing Risk	Description
Compliance Risk	The risk arising from violations of laws, rules, regulations, or from noncompliance with the RFI's internal policies or procedures or business standards. This risk exists when the products or activities of a service provider are not consistent with governing laws, rules, regulations, policies, or ethical standards. Some examples include: • Third parties may engage in deceptive product marketing practices or discriminatory lending practices that are in violation of applicable laws and regulations.

Inherent Outsourcing Risk	Description
	• The ability of the service provider to maintain the privacy of customer records and to implement an appropriate information security and disclosure program.
Country Risk	The exposure to the economic, social and political conditions and events in a foreign country that may adversely affect the ability of a cross border third-party service provider (CBSP) to meet the level of service required by the arrangement, resulting in harm to the RFI. In extreme cases, this exposure could result in the loss of data, research and development efforts, or other assets.
Cyber Risk	Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems. RFI's may not sufficiently understand or have control over the third party provider's cyber protection procedures, and the third party provider may not notify the client in a timely manner when a breach occurs. RFIs may be exposed to data breach losses as a result of cyber breaches.
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events. Third-party relationships often integrate the internal processes of other organizations with the RFI's processes and can increase the overall operational complexity. RFIs should be cautious about outsourcing services from a service provider that supplies services to multiple RFIs as operational risks are correspondingly concentrated and may pose a systemic threat.
Reputation Risk	The risk arising from negative public opinion. Third-party relationships that result in dissatisfied customers; unexpected customer financial loss; inconsistent interactions with the RFI's policies; inappropriate recommendations; security breaches resulting in the disclosure of customer information; and violations of laws and regulations are all examples that could harm the reputation and standing of the RFI. Any negative publicity involving the service provider, whether or not the publicity is related to the RFI's use of the service provider, could result in reputation risk.
Strategic Risk	The risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the RFI's strategic goals. Where a service provider does not adequately perform services that assist the RFI in achieving its corporate strategic goals nor provides an adequate return on its investments, it exposes the RFI to strategic risk.
Transaction Risk	The risk arising from problems associated with service or product delivery. A third-party's failure to perform as expected by customers or the RFI due

Inherent Outsourcing Risk	Description
	to inadequate capacity, technological failure, human error, or fraud, exposes the RFI to transaction risk. The lack of effective business contingency plans increases transaction risk. Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources. These issues could result in unauthorized transactions or the inability to transact business as expected.

5.3 Principle 3 - Access

RFIs should ensure that outsourcing neither diminishes their ability to fulfill their obligations to customers and the Central Bank, nor impedes effective supervision by the Central Bank. The RFI should therefore ensure that:

5.3.1 There is proper monitoring and control of the outsourced activity or service. Material outsourcing contracts should include provisions, which allow the RFI the right to monitor and conduct periodic reviews to verify that the service provider is in compliance with the terms of the contract, or alternatively, to cause an independent auditor to evaluate, on its behalf, the service provider's internal control environment and risk management practices. The contract should also allow the RFI, in specified circumstances, access to internal and external audit reports prepared on the service provider in respect of the outsourced activity, function, process or service

5.3.2 Where the service provider has access to any confidential data, the provisions within the contract should prohibit the inappropriate use or disclosure of such information.

5.3.3 The outsourcing contract permits the RFI to require remedial or corrective action by the service provider for issues that arise which compromise the integrity of the activity being provided or where non-compliance with applicable laws and regulations, as well as, non-compliance with terms of the contract is detected.

5.3.4 The outsourcing does not impair the Central Bank's ability to exercise its regulatory responsibilities:

a) Therefore, the RFI should include, as a condition in the outsourcing contract, the ability of the Central Bank to request an examination or audit of the service provider, which will be undertaken by the RFI or an independent auditor. An examination or audit of the service provider under these circumstances would be specific to the service provider's activities as it relates to the outsourcing arrangement with the RFI.

b) The Central Bank should be granted access to internal and external audit reports prepared on the service provider in respect of the outsourced activity, function, process or service.

c) The RFI is to ensure that the outsourcing contract does not impair its ability to access all books, records, and information on the outsourced activity, function or service. All such information should be accessible to the Central Bank[3] upon request, whether held by the RFI or service provider.

5.3.5 The RFI shall ensure that outsourcing arrangements do not create impediments to the resolvability of the institution.

5.4 Principle 4 – Due Diligence

RFIs should conduct appropriate due diligence in selecting a service provider.

5.4.1 Adequate criteria should be established that enables the RFI to assess, prior to selection, the service provider's capacity and ability to perform the outsourced activities effectively, reliably and to a high standard. The criteria must be included in the outsourcing policy, which is to be board approved.

5.4.2 Due diligence processes will vary depending on the RFI and on the nature of the outsourcing arrangement being contemplated. However, particularly in the case of material outsourcing arrangements, the due diligence of the service provider, should include *inter alia* a review of:

a) the experience and the technical competence of its management and relevant staff to implement and support the proposed activity;
b) the security, technological and internal controls, reporting and monitoring environment including its ability to adequately maintain confidentiality of information;
c) its financial soundness and ability to service commitments;
d) its business reputation and culture, for example consideration of complaints and pending litigation where appropriate;
e) its business goals, objectives, continuity management and strategies;
f) laws and regulations of the service provider's jurisdiction (where applicable);
g) whether a licence will be required to conduct the outsourced activities;

[3] Section 78 (1) (a) of the Financial Institutions Act, 2008 grants the Central Bank the power to request information from "an agent" of a licensee. A service provider would be considered an agent of the RFI. . Section 11(1)(a) of the IA also provides that the Inspector may request information from any person acting on behalf of a FHC, insurer, agency or brokerage, which would include a service provider acting on behalf of an RFI in relation to an outsourced activity. Section 10(12) of the IA and 62(14) of the FIA provide that the Central Bank shall have access to, *inter alia*, all books, records and any other documents (including those stored in electronic form) of a registrant/licensee or FHC, even where in the possession of another person.

h) whether the principals and the company are designated or sanctioned persons on any applicable list issued by the United Nations Security Council or identified by the courts of Trinidad and Tobago as terrorist entities; and
i) any other relevant information.

5.4.3 In its ongoing due diligence, the RFI should be able to monitor the service provider's performance and compliance with its contractual obligations. To achieve this, the RFI should establish:

a) clearly defined metrics to monitor the service provider, specify what service levels are required and measure the efficiency and effectiveness of the service provider against these metrics; and

b) clear criteria as to what constitutes instances of non-compliance or unsatisfactory performance by the service provider. Quality assessment of services provided by the service provider should also be conducted at specified intervals and clearly documented.

5.5 Principle 5 – Written Contracts

All material outsourcing relationships should be governed by written contracts that clearly describe all key aspects, such as the nature and scope of the service being provided and including the rights, responsibilities and expectations of all parties.

5.5.1 The contract should be sufficiently flexible to allow for renegotiation and renewal to enable the RFI to retain an appropriate level of control over outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. Therefore, key provisions of the outsourcing contract should include *inter alia*:

a) Limitations or conditions, if any, on the service provider's ability to subcontract. However, where subcontracting is permitted, it should require the prior consent of the RFI and any obligations pertaining to the subcontract should be clearly stipulated, in particular, the security and confidentiality standards that should apply to subcontracting or outsourcing arrangements by the primary service provider and the service provider's due diligence process for engaging and monitoring subcontractors. Additionally, the primary service provider must remain responsible for all of its obligations under the agreement. When assessing whether to approve a subcontractor, the RFI is expected at a minimum, to consider if it can maintain a similar control over the risks when a service provider outsources to the subcontractor as in the original direct outsourcing arrangement.

b) Requirements that the service provider comply with the same (or higher) standards as those that the RFI with respect to IT, security, confidentiality and disclosure of all information relating to or obtained from the RFI;

c) Insurance and indemnities;

d) Obligation of the service provider to provide, upon request, records, information and/or assistance concerning the outsourcing arrangements to the RFI's auditors and/or its regulators;

e) Mechanisms to resolve disputes that might arise under the outsourcing arrangement;

f) Business continuity provisions;

g) Examples of the type of events/adverse developments and the circumstances under which the service provider should report to the RFI in order for the RFI to take prompt risk mitigation measures;

h) Provisions for the termination of the contract, transfer of information and exit strategies; and

i) Responsibility of the service provider for compliance with local laws and regulations as required.

5.5.2 The **minimum elements** to be included in an outsourcing contract or agreement are detailed in **Appendix 3** of this Guideline.

5.5.3 Material outsourcing contracts should also adhere to and be compliant with all applicable laws of this jurisdiction.

5.6 Principle 6 – Business Continuity and Contingency Plans

RFIs and their service providers should establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.

5.6.1 Business continuity and contingency plans should be included in material outsourcing contracts, and should specify the service provider's measures for ensuring the continuation of the outsourced services or activities in the event of problems such as a system breakdown or natural disaster that may affect the service provider's operation. Provisions should also be included in the contract for transfer of the RFI's activities to another service provider without penalty, in the event of the service provider's bankruptcy or business failure.

5.6.2 Specific contingency plans should be developed separately for each material outsourcing arrangement. Notably, the RFI should consider contingency plans at

the service provider; co-ordination of contingency plans at both the RFI and the service provider; and contingency plans of the RFI in the event of nonperformance.

5.6.3 Back-up arrangements should be tested at least annually by the service provider and the results provided to the RFI, together with any significant changes in the business resumption plan. The service provider should inform the RFI of material changes to their business continuity plans.

5.6.4 There are also risks where multiple service providers depend on the same provider of business continuity services with a common disaster recovery site. Any disruption that affects a large number of service providers may result in a lack of capacity for the business continuity services. The RFI should therefore be able to undertake at least one of the following exit strategies, within an appropriate timeframe:

a) transfer the function to an alternative service provider;

b) reintegrate the function; or

c) discontinue the business activities that are depending on the function.

5.7 Principle 7 – Confidentiality

RFIs should take appropriate steps to require that service providers protect the confidential information of both the RFI and its clients from intentional or inadvertent disclosure to unauthorized persons.

5.7.1 The RFI must take appropriate steps to prevent the disclosure of confidential information to unauthorized persons by service providers. For example, the RFI should ensure that the service provider implements appropriate security measures to safeguard all confidential information, taking into account any regulatory or statutory provisions that may be applicable.

5.7.2 The RFI should be proactive in identifying and specifying requirements for confidentiality, security, and disclosure in the outsourcing arrangements.

5.7.3 Any transfer of customer information from the RFI to a third party service provider under the terms of an outsourcing contract should be with the customer's consent. Such consent may be obtained at the initiation of the customer/RFI relationship as a term of the customer agreement or alternatively, prior to the proposed transfer of information. The rights of customers should not be affected because of the outsourcing arrangement between the service provider and the RFI.

5.7.4 Appropriate data confidentiality, security, and separation of property provisions should be included in the outsourcing contract.

5.7.5 The RFI should notify the Central Bank of any adverse development arising from its outsourcing arrangement, which affects the RFI or its customers including any unauthorized access or breach of confidentiality by the service provider (or its sub-contractors).

6. BUSINESS ACTIVITIES / SERVICES THAT SHOULD NOT BE OUTSOURCED

6.1 Ideally, RFIs should not outsource certain core management functions pertaining to internal controls, compliance, and decision-making functions. However, RFIs are permitted to implement intra-group outsourcing arrangements within a financial group structure, subject to the risk management principles established in this Guideline. RFIs shall not outsource the following activities to persons outside the financial group:

6.1.1 Corporate planning, strategic planning, risk management, and internal controls;

6.1.2 Regulatory obligations in respect of the Money Laundering / Financing of Terrorism / Proliferation Financing (ML/TF/PF) control function, pertaining to the assessment of the ML/TF/PF risk and the determination of whether to report the matter to any authority remain the responsibility of the RFI. Operational activities supporting the risk assessment and decision making, such as the collection of Know Your Customer (KYC) information, transaction monitoring or screening against lists may be outsourced; and

6.1.3 Loan approvals.

6.2 The RFI remains ultimately responsible and accountable to the Central Bank and the customer for any error or breach by the service provider in all of its outsourcing contracts.

7. OUTSOURCING ARRANGEMENTS WITH AN EXTERNAL AUDITOR

7.1 The RFI may at times outsource certain non-audit services to its external auditor. Non-audit services performed by external auditors fall into two main categories:

7.1.1 Services considered most efficient for the external auditors to provide because of their existing knowledge of the business, or because the information required is a by-product of the audit process. These include services where the information largely derives from the audited financial records; tax compliance; reports required in acquisition or reorganization situation where completion is necessary in a short timeframe.

7.1.2 Consultancy services such as management consultancy, tax advice, and human resources consultancy.

7.2 Where non-audit services are outsourced to its external auditor, the RFI is required to ensure that such arrangements are conducted at an arm's length basis to avoid conflicts of interest.

7.3 Notwithstanding, 7.1, there are certain non-audit services that cannot be outsourced to the RFI's current external auditor[4] responsible for its annual audit. Such non-audit services include:

7.3.1 Actuarial services unless it is reasonable to conclude that the results of the service will not be subject to audit procedures during an audit of the RFI's financial statement;

7.3.2 Internal audit services related to the internal accounting controls, AML/CFT compliance, financial systems, or financial statements of the RFI, unless it is reasonable to conclude that the results of the service will not be subject to audit procedures during an audit of the RFI's financial statements. This does not prohibit the external auditor from providing a non-recurring service to evaluate a discrete item or program, if the service is not, in substance, the outsourcing of an internal audit function;

7.3.3 Book-keeping or other services related to its accounting records or financial statements;

7.3.4 Financial information systems design and implementation services; and

7.3.5 Such other non-audit related services as the Central Bank may from time to time prescribe.

8. MATERIAL INTRA-GROUP OUTSOURCING ARRANGEMENTS

8.1 While the Central Bank expects the RFI to follow or adhere to all of the principles detailed in this guideline as it pertains to intra-group outsourcing, reduced expectations may be applied to such outsourcing relationships.

8.2 At a minimum, the Central Bank expects the following to be addressed when a material outsourcing arrangement is entered into with another entity that is a member of the same financial group:

8.2.1 An outsourcing or service level agreement that details, among other things, the scope of the arrangement, the services to be supplied, the nature of the relationship

[4] See section 81(9) of the FIA and section 75(6) of the IA.

between the RFI and the service provider and procedures governing the sub-contracting of services;

8.2.2 An appropriate business continuity plan;

8.2.3 A process for monitoring and oversight; and

8.2.4 Establishment of terms and conditions that will allow the Central Bank to properly monitor and regulate the RFI's outsourced activity. This includes ensuring that the Central Bank is able to access all information, books, and records pertaining to the outsourced activity, function or service, upon request.

9. OUTSOURCING TO A CROSS-BORDER SERVICE PROVIDER (CBSP)

9.1 The RFI should closely monitor government's policies and political, social, economic and legal conditions in countries where the service provider is based and establish sound procedures for dealing with country risk for **all cross-border outsourcing arrangements**, whether material or not. RFIs can face significant adversity from foreign political, economic and social conditions in other countries, which may negatively affect the service provider's ability to service the outsourcing arrangement.

9.2 In addition to the assessment that would be conducted for a local outsourcing provider and the requirements for written outsourcing contracts in Principle 5.5, RFIs engaged in any outsourcing arrangements with a CBSP should:

9.2.1 In principle, enter into arrangements only with service providers operating in jurisdictions with an equivalent (or higher) standard of data protection and privacy legislation, regulation or supervision as exists in Trinidad and Tobago;

9.2.2 Clearly specify the governing law of the arrangement;

9.2.3 Ensure that the outsourced activity is conducted in a manner so as not to hinder efforts to supervise or reconstruct the Trinidad and Tobago activities of the RFI (that is, from its books, accounts and documents) in a timely manner; and

9.2.4 Notify the Central Bank if any overseas authority was to seek access to its customer information, or if a situation was to arise, where the rights of access of the RFI and the Central Bank have been restricted or denied.

9.3 The RFI is expected to conduct a more rigorous assessment of an overseas service provider given the higher level of risk exposure. This evaluation, in addition to what would be done for a local provider, would include:

9.3.1 Conducting a risk assessment, which includes the monitoring of economic, social, and political conditions as well as government policies within the foreign jurisdiction;

9.3.2 Assessing the CBSP's ability to meet the RFI's needs, given the laws, regulatory requirements, local business practices, accounting standards and legal environment in the foreign jurisdiction; and

9.3.3 Examining the operational risks as it relates to security and confidentiality of the RFI and customers' information. The RFI should ensure that the confidentiality of customer information is in accordance with relevant laws and the provisions in the contract between the customer and the RFI.

10. CLOUD COMPUTING

10.1 The use of cloud computing services by RFIs is increasing in today's fast evolving technological environment. This section provides additional guidance in the specific context of institutions that outsource to cloud service providers.

10.2 RFIs are reminded that cloud computing service providers routinely utilize global distribution of data processing and storage, which may increase exposure to particular risks. RFIs should therefore take special care when entering into and managing outsourcing agreements undertaken outside Trinidad and Tobago because of possible data protection risks and risks to effective supervision by the Central Bank. In considering the outsourcing of cloud computing services, RFIs must be prepared to address data issues surrounding accessibility, confidentiality, integrity, sovereignty, recoverability and regulatory compliance. The Central Bank expects RFIs to implement effective measures to address these issues.

10.3 RFIs must ensure that prior to engaging cloud computing service providers, all data, services and/or processes, which will be impacted, are identified and assessed in order to establish readiness. RFIs should therefore adopt a risk-based approach to data and data processing location considerations when outsourcing to a cloud environment. The assessment should address the potential risk impacts, including legal risks and compliance issues, and oversight limitations related to the countries where the outsourced services are or are likely to be provided and where the data are or are likely to be stored.

10.4 It is important that in evaluating cloud computing service providers, RFIs also identify and liaise with all of their relevant internal stakeholders including but not limited to the following departments: Information Technology (enterprise architecture and information security), Risk, Compliance, Finance and Legal.

11. ROLE OF THE CENTRAL BANK

11.1 As part of its supervisory framework, the Central Bank will evaluate the implementation of the principles detailed in this Guideline. In the event that deficiencies are identified during routine monitoring, onsite examinations, or through the review of documents provided, the Central Bank will address these issues with the RFI directly and may require the RFI to take additional measures to address the deficiencies noted.

12. EFFECTIVE DATE AND TRANSITION PERIOD

12.1 This Guideline is effective from the date of issuance but recognizes that transition periods are necessary as it may not be possible to amend existing contracts. Therefore, RFIs, which have existing outsourcing contracts, are required to:

12.1.1 Review all current material outsourcing contracts to assess compliance with this Guideline; and

12.1.2 Notify the Inspector of Financial Institutions ("Inspector"), within six (6) months of the issuance of this Guideline, of **all existing material** outsourcing contracts using Appendix 2.

12.2 RFIs are expected to take the necessary steps to ensure that at a minimum, material outsourcing contracts adhere to this Guideline at the earliest opportunity, or institute measures to mitigate identified risks where the contract cannot be amended in a reasonable timeframe.

12.3 Consequently, **material** outsourcing contracts:

12.3.1 that are expiring within 18 months of the date of issuance of this Guideline may continue unchanged;

12.3.2 that are expiring after 18 months of the date of issuance of this Guideline should be reviewed to determine whether amendments can be made to the contract to facilitate compliance with the Guideline.

12.4 New contracts being entered into post issuance of this Guideline must consider and adhere to the requirements in this Guideline.

12.5 Outsourcing arrangements that an RFI has obtained as a result of an acquisition are expected to comply with the expectations set out in the Guideline at the first opportunity, such as the time the outsourcing contract, agreement or statement of work (where applicable) is substantially amended, renewed or extended.

12.6 Where the revision of any material contract referred to in 12.3.2 and 12.5 is not possible, the Inspector must be notified and provided with an explanation as well as a plan to manage and mitigate any identified risks.

APPENDIX 1 –

EXAMPLES OF COMMONLY OUTSOURCED ACTIVITIES & SERVICES

- Information system management and maintenance (e.g. data entry and processing, data centres, facilities management, end-user support, local area networks, help desks);
- Document processing (e.g. cheques, credit card slips, bill payments, bank statements, other corporate payments);
- Application processing (e.g. insurance policies, loan originations, credit cards);
- Policy administration (e.g. premium collection, policy assembly, invoicing, endorsements);
- Claims administration (e.g. loss reporting, adjusting);
- Loan administration (e.g. loan processing, collateral management, collection of bad loans);
- Investment management (e.g. portfolio management, cash management);
- Marketing and research (e.g. product development, data warehousing and mining, advertising, media relations, call centres, telemarketing);
- Back office management (e.g. payroll processing, custody operations, quality control, purchasing);
- Real estate administration (e.g. building maintenance, lease negotiation, property evaluation, rent collection);
- Professional services related to the business activities of the RFI (e.g. accounting, internal audit, actuarial); and
- Human resources (e.g. benefits administration, recruiting).

This Guideline generally would not apply to the following:

- Courier services, regular mail, utilities, telephone;
- Procurement of specialized training;
- Discrete advisory services (e.g., legal opinions, certain investment advisory services that do not result directly in investment decisions, independent appraisals, trustees in bankruptcy);
- Purchase of goods, wares, commercially available software and other commodities;
- Independent audit reviews;
- Credit background and background investigation and information services;
- Market information services (e.g., Bloomberg, Moody's);
- Independent consulting;

- Services the RFI is not legally able to provide;
- Printing services;
- Repair and maintenance of fixed assets;
- Supply and service of leased telecommunication equipment;
- Travel agency and transportation services;
- Correspondent banking services;
- Maintenance and support of licensed software;
- Temporary help and contract personnel;
- Fleet leasing services;
- Specialized recruitment;
- External conferences;
- Clearing and settlement arrangements between members or participants of recognized clearing and settlement systems;
- Sales of insurance policies by agents or brokers;
- Ceded insurance and reinsurance ceded; and
- Syndication of loans.

APPENDIX 2 –

TEMPLATE OF CENTRALIZED LIST OF OUTSOURCED SERVICES

Name of Service Provider	Name of Service Provider's Parent Company (if applicable)	Brief description of the Outsourced Service	Indicate materiality level of the outsourced service to the RFI or Financial Group (i.e. Low/Moderate/ High)	Service Provider's Jurisdiction of Incorporation	Applicable laws Governing the contract	Date Contract entered into	Expiry/Renewal date of contract or outsourcing agreement	Estimated annual spending on arrangement	Estimated $ Value of contract or outsourcing agreement

APPENDIX 3 –

MINIMUM ELEMENTS OF OUTSOURCING CONTRACTS

1. Nature and scope of the service being outsourced to the service provider. (Section 5.5)
2. Service level and Performance Standards – e.g. timing of delivery; metrics to measure performance; procedures for managing problems. (Section 5.4.3)
3. Ownership and Access – e.g. ownership of assets; rights of the access of the service provider to RFI's assets etc. (Section 5.3.2)
4. Fees
5. Insurance and Indemnities (Section 5.5.1(c))
6. Reporting Requirements – e.g. the type and frequency of reporting by the service provider. (Sections 5.3.1 and 5.5.1(d))
7. Audit and Examination Rights – e.g. rights of the RFI to audit the service provider or appoint an auditor to do same; rights of the Central Bank request an audit of the service provider; rights of access by the RFI and the Central Bank to any reports on the service provider by its internal or external auditors. (Sections 5.3.3 and 5.3.5)
8. Business Continuity Plans (Section 5.6)
9. Default and Termination of the Contract (Section 5.5.1(g))
10. Dispute Settlement (Section 5.5.1(e))
11. Documentation/ Information Retention (Sections 5.3.5 and 5.5.1(d))
12. Confidentiality, Data Protection and Security of Customer Information (Sections 5.5.1(b) and 5.7)
13. Sub-Contracting (if applicable) (Section 5.5.1(a))
14. Examples of the type of events/adverse developments and the circumstances under which the service provider should report to the RFI in order for the RFI to take prompt risk mitigation measures (Section 5.5.1 (g))

This list is not considered exhaustive and the Central Bank may amend it periodically.