GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$20.00 WINDHOEK - 23 June 2022 No. 7835

CONTENTS

Page

General Notice

BANK OF NAMIBIA

No. 286 2022

DETERMINATION UNDER THE BANKING INSTITUTIONS ACT, 1998
(ACT NO. 2 OF 1998), AS AMENDED:
OUTSOURCING IN BANKING INSTITUTIONS AND CLOUD COMPUTING

In my capacity as Governor of the Bank of Namibia (Bank), and under the powers vested in the Bank under section 71(3) of the Banking Institutions Act, 1998 (Act No. 2 of 1998), I hereby issue this Determination on the Outsourcing in Banking Institutions and Cloud Computing (BID-34).

J. !GAWAXAB
GOVERNOR

Determination No. BID-34

OUTSOURCING IN BANKING INSTITUTIONS AND CLOUD COMPUTING

Arrangement of paragraphs

PART I

PRELIMINARY

PARAGRAPH

PART II

STATEMENT OF POLICY

PART III

IMPLEMENTATION AND SPECIFIC REQUIREMENTS

PART IV

EFFECTIVE DATE

19. Effective date

ANNEXURES

ANNEXURE A

ANNEXURE B

PART I: PRELIMINARY

1. **Short Title** – Outsourcing and Cloud Computing

2. **Authorisation** – Authority for the Bank to issue this Determination is provided in terms of section 71(3) of the Banking Institutions Act, 1998 (Act No. 2 of 1998), as amended.

3. **Application** – This Determination applies to all banking institutions authorised by the Bank to conduct banking business in Namibia.

4. **Definitions** – Terms used in this Determination are defined in the Act, and further defined below, or as reasonably implied by the contextual usage.

4.1 **"Act"** means the Banking Institutions Act, 1998 (Act No. 2 of 1998) as amended;

4.2 **"Bank"** means the Bank of Namibia as referred to in section 2 of the Bank of Namibia Act, 2020 (Act No. 1 of 2020);

4.3 **"cloud-based services"** or **"cloud computing"** refers to the set of on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage facilities, applications and services). Such resources can be rapidly provisioned and released with minimal management effort or service provider interaction:

a) **Software as a Service (SaaS)** means using general software or business-specific applications run on computers in the cloud but owned and operated by the cloud service providers;

b) **Platform as a Service (PaaS)** means a using complete computer environment that is provided for building and delivering web-based applications (be they internally developed or acquired applications) while the cloud service provider undertakes the purchase, management and hosting of the underlying hardware;

c) **Infrastructure as a Service (IaaS)** means companies are provided computing resources, including servers, networking, storage, and data centre space.

Cloud resources may be provided through public, private, community or hybrid cloud deployment models:

d) **public cloud** refers to services and infrastructure owned and operated by the service providers and offered off-site over a public network;

e) **private cloud** refers to services and infrastructure operated solely for a single organisation, whether managed internally or by a third party and hosted on a private network;

f) **community cloud** refers to cloud infrastructure available for exclusive use by a specific community of institutions, including several institutions within a single group; and

g) **hybrid cloud** refers to services built on a private cloud foundation with a combination of public cloud services.

4.4 **"core business activities or functions"** refer to business activities or functions which cannot be outsourced;

4.5 **"critical shared services"** means any activities or functions, whether performed internally or outsourced, that support a banking institution's critical functions and where a failure of such services would lead to a failure or disruption of critical functions;

4.6 **"insourcing"** refers to functions or business activities which have been outsourced to a third-party service provider within a particular group of institutions that form part of a single banking group;

4.7 **"material business activities"** means business activities or functions of such importance that have a significant impact on the banking institution's business operations, its ability to manage risks effectively or its continued regulatory compliance should such activities be disrupted;

4.8 **"non-material business activities"** means business activities or functions that do not affect the internal control system (including the systems, policies, procedures, and processes implemented by a banking institution to safeguard its assets, limit or control risk) and do not pose a significant risk to the operation of a banking institution;

4.9 **"offshoring"** means the outsourcing by a banking institution of a material business activity or function to a third-party service provider who conducts the outsourced activity or function outside the borders of Namibia. All references to cloud computing arrangements include offshoring arrangements;

4.10 **"outsourcing"** – means the use of a service provider, whether it is an affiliate within a corporate group or a third party, to perform a business activity, service, function or process, which could be undertaken by the banking institution, on behalf of the banking institution;

4.11 **"outsourcing arrangement"** - means a written, legally binding agreement between a banking institution and a third party service provider, where a third party service provider performs a business activity, function or process that the banking institution itself could ordinarily undertake;

4.12 **"third-party service provider"** – means an entity that is undertaking the outsourced function or activity on behalf of the banking institution and includes members of the corporate group to which the banking institution belongs or an entity that is external to the banking group, whether located in Namibia or elsewhere.

PART II: STATEMENT OF POLICY

5. **Purpose** – This Determination sets out the requirements that a banking institution must observe in assessing and managing risks relating to outsourcing relationships, including cloud computing arrangements.

6. **Scope** – This Determination guides all aspects relating to outsourcing business activities or functions, including cloud computing arrangements of a banking institution.

PART III: IMPLEMENTATION AND SPECIFIC REQUIREMENTS

7. **Responsibility**

7.1 The board of directors of a banking institution is responsible for ensuring compliance with this Determination and for ensuring, at a minimum, that:

a) An outsourcing policy that comprehensively guides the assessment and risk management of outsourced activities or functions is approved by the Board of Directors and reviewed at least triennially.

b) The risks associated with outsourced activities or functions are identified and duly managed to ensure that a banking institution delivers on its obligations. These outsourced activities or functions include insourcing and cloud computing arrangements.

c) A banking institution has comprehensive risk management, internal control and oversight processes, practices and procedures to manage various outsourcing arrangements.

d) Outsourced activities or functions are conducted safely and soundly and in compliance with the applicable legislation. Where compliance issues are identified, these are to be comprehensively and timeously addressed by the banking institution in conjunction with relevant risk and compliance functions.

e) The Bank and the banking institution's external auditors have access to information relating to the outsourced function or activity to enable them to execute their duties under the Act and other relevant legislation.

7.2 Senior management is required to ensure the following key requirements relating to outsourcing of material business activities and functions are in place:

a) A plan for assessing outsourcing strategies and arrangements and evaluating their consistency with and supporting the banking institution's strategic objectives is established.

b) A programme for outsourcing activities or functions, including performing risk assessments surrounding the outsourcing of material business activities and functions both before entering into the arrangement and during the arrangements, and determining appropriate approval mandates for outsourced services.

c) A comprehensive risk assessment and risk mitigation strategies to address the risks associated with outsourced arrangements with third party service providers. The risks should be periodically reassessed in line with the banking institution's risk management framework.

d) Notify the Bank before outsourcing material business activities and functions per paragraph 8.

e) Ensure that a senior official within the banking institution is specifically designated the responsibility of managing outsourced services and is accountable for the smooth operating of the outsourced function or activity and compliance of the third party service provider with this Determination where applicable. This official should be competent and adequately authorised to make decisions commensurate with the nature, scope and complexity of the outsourcing arrangements.

f) Monitor the regulatory and compliance landscape for change and, where applicable, consider all respective regulations when considering all outsourcing and cloud computing arrangements to ensure compliance. A banking institution should be aware that regulators in other jurisdictions may impose additional requirements on the banking institution in addition to local legislative requirements.

g) Should be aware of the legislative requirements applicable to the third party service provider in the countries where the banking institution's data is hosted and determine whether this does not impose undue risk on the banking institution, especially where countries have rights to seize or otherwise access data hosted by the third party service providers.

7.3 A banking institution remains accountable for compliance with all legislative requirements. Therefore, it should ensure that a contractual agreement with third party service providers incorporates the necessary arrangements that will enable them to remain compliant. It further remains the responsibility of each banking institution to evidence such compliance.

8. Material business activities and functions

8.1 A banking institution must possess an outsourcing policy that comprehensively guides the identification and classification of outsourced functions and business activities to determine the materiality of each function or business activity. The following factors should be considered in determining the materiality of business activity or function:

a) The financial and operational impact should the business activity or function be interrupted or cease.

b) The reputational impact should the third party service provider fail to perform the outsourced activity or function over a given period.

c) The cost of the outsourcing arrangement as a percentage of total expenses.

d) The degree of difficulty, including the time taken, in finding an alternative third party service provider or bringing the business activity or function in-house.

e) The affiliation or other relationship between the banking institution and the third party service provider. As well as the number and value of outsourcing arrangements held with one service provider, which in totality may be deemed material to the banking institution.

f) The banking institution's ability to maintain appropriate internal controls and meet regulatory requirements continuingly, including problems with the third party service provider.

g) The effect of the outsourcing arrangement on the supervisory processes of the Bank.

h) The impact on the banking institution's strategic objectives should the third party service provider fail to perform its activity or function in terms of the outsourcing arrangement.

i) The nature and/or value of potential losses to the banking institution and its customers in the event of a third party service provider's failure to perform per the outsourcing arrangement.

8.2 A banking institution is required to identify and duly classify outsourced business activities and functions as:

a) Core activities – business activities or functions which may not be outsourced;

b) Material activities – business activities or functions which may be outsourced with prior notification of the Bank; and

c) Non-material activities – business activities or functions which may be outsourced with no notification of the Bank.

8.3 The Bank views management oversight, governance, risk management and compliance as material business activities or functions can only be insourced with the written approval of the Bank.

8.4 The Bank considers internal audit as a material business activity or function which can only be outsourced with the written approval of the Bank.

8.5 The Bank regards critical shared services, including insourced arrangements, as material business activities or functions which should only be insourced with prior written notification to the Bank.

8.6 The Bank does not permit the outsourcing of data centres hosting production core banking IT systems as this is viewed as a core business activity or function.

a) To this end, a banking institution must locate their data centres, hosting their production core banking systems, on local infrastructure. Local IaaS for the production core banking system may be considered on a case-by-case basis with the written approval of the Bank.

b) A banking institution may elect to locate their data centre hosting replicated or backup copy of the core banking system on an infrastructure owned, hosted and administered by the parent company only. This arrangement requires prior written notification to the Bank.

c) All non-core banking systems must be categorised as material or non-material IT systems and may be outsourced, i.e., cloud computing arrangements, per the requirements of this Determination.

d) This Determination does not supersede the Determination on the Localisation of Core Banking Systems (BID-19).

8.7 Where written notification is required, a banking institution must ensure the notification includes supporting documentation on the outsourced activity and vendor to the satisfaction of the Bank. Supporting documentation includes due diligence, selection criteria, contractual agreement, Service Level Agreement at a minimum.

9. Non-Material outsourced Activities and Functions

9.1 Outsourced functions or activities which are assessed and designated as non-material include those which do not affect the internal control system of a banking institution, do not pose a significant risk to operational continuity and fall outside of the criteria for material outsourced arrangements. Banking institutions are required to notify the Bank where non-material activities or functions become material activities or functions.

9.2 A banking institution is not required to notify the Bank under this Determination to outsource non-material activities or functions. However, a banking institution is required to ensure that adequate risk management is exercised at all times and oversight is exercised by the board and senior management over these activities or functions. The outsourcing policy should clearly indicate how non-material outsourcing activities and functions will be managed.

10. Insourcing

10.1 The Bank requires insourced arrangements of a banking institution to be prudently and comprehensively managed in a manner similar to any other third party sevice provider. To this end, the selection and management of a group entity are subject to the requirements of this Determination. Such arrangements must thus be based on objective reasons, the conditions of the outsourcing arrangement set at arm's length, explicitly deal with conflict of interest, not impair the banking institution's ability to comply with regulatory requirements and fees levied be documented, transparent and commensurate with service rendered.

10.2 All notifications for insourced activities referenced under paragraphs 8.3 and 8.5 above must be accompanied by documentation supporting the due diligence, selection criteria, contractual agreement and Service Level Agreement of the third party provider.

10.3 The insourcing arrangement must clearly detail the pricing methodology and cost components for any fees charged for insourced activities or functions. A detailed and comprehensively granular invoice must be provided to each banking institution justifying the fees charged.

10.4 All existing insourced arrangements must be brought into compliance with the requirements of this Determination. Transfer pricing across legal entities is also considered insourcing for the purpose of this Determination.

11. Outsourcing policy

11.1 A banking institution must have a Board approved outsourcing policy that addresses the identification, classification, assessment, management, mitigation and reporting of risks associated with outsourcing. The banking institution should ensure compliance with the policy by all concerned parties, including the third-party service provider.

11.2 The outsourcing policy should establish an outsourcing risk management programme that addresses risk assessments and due diligence, ongoing monitoring of service providers, and business continuity and contingency planning. The programme should also address the integration of outsourcing arrangements within the banking institution, the importance and adequacy of internal expertise and management frameworks to oversee and manage the outsourced activity or function and the relationship with the third party service provider, and the business case for outsourcing a material business activity or function.

11.3 The outsourcing policy should include:

a) The strategic goals, objectives and business needs of the banking institution in relation to outsourcing.

b) Clear definitions of the range of activities or functions that may be outsourced and those activities or functions which may not be outsourced.

c) Limits on and appetite for the overall acceptable level of outsourced activities or functions within the banking institution and limits on the geographical location of a third party service provider, if applicable.

d) Criteria for the classification process for designation of outsourced activities or functions as core, material and non-material, including cloud computing.

e) Eligibility criteria for selecting third party service providers taking into account any relation, directly or indirectly, with the banking institution.

f) Processes and criteria for evaluating and reporting on the risks and controls associated with outsourced activities or functions of varying natures on an ongoing basis.

g) Issues that address risk concentration and risks arising from outsourcing multiple activities or functions to the same third party service provider or multiple banking institutions using the same third party service provider.

h) Steps to ensure compliance with legal and regulatory requirements in both home and host countries.

i) The assessment and assurance to be obtained regarding third party service provider contingency plans to ensure operational continuity in case of business disruption.

12. Planning and risk assessments

12.1 A banking institution should develop a plan to manage outsourcing relationship. The risk management plan should be proportionate to the level of risk and complexity of the relationship between a banking institution and a third party service provider. The risk measurement and management plan should be commensurate with the nature, scope, scale and degree of complexity of the banking institution's operation.

12.2 A banking institution should consider its ability and expertise to provide appropriate oversight and management of the relationship with the third party service provider. The risk assessment should be updated as part of monitoring and managing the outsourcing relationship. In addition, the banking institution should update its risk mitigation plans based on the results of the risk assessment.

12.3 The senior official within the banking institution designated the responsibility and accountability for managing each outsourced arrangement is responsible for ensuring the risk assessments, due diligence, contracting, and monitoring of third party service providers is managed prudently and per this Determination.

13. Due diligence and selection

13.1 A banking institution should conduct the necessary due diligence on a prospective third party service provider before entering into an outsourcing agreement, including insourced agreements.

13.2 When performing due diligence, a banking institution should, amongst others, consider the following factors about the third-party service provider:

a) Scope, complexity and materiality of the business activity or function;

b) Business background, business activities, and the reputation and industry standing of the service provider;

c) Financial performance and condition;

d) Human resources management;

e) Qualifications, backgrounds and reputations of company principals;

f) Risks involved in the outsourcing arrangement and risk management of third-party service provider;

g) Incident reporting and management programmes;

h) Information security;

i) Insurance coverage;

j) Jurisdictional considerations and sovereign risks;

k) Legal and regulatory compliance of third party service provider at the time of assessment and of banking institution following commencement of the outsourcing arrangement;

l) Management of information systems, data security and storage of banking institution data (e.g. format, location and period);

m) Operations and internal controls;

n) Physical security;

o) Use of and reliance on subcontractors;

p) Vendor concentration and systemic risk[1].

13.3 A banking institution should consider the following requirements when assessing its outsourcing options:

a) Prepare and consider an appropriate business case;

b) Undertake a tender or other selection process for third party service providers;

c) Undertake a due diligence review of the chosen third party service provider;

d) Involve the board, board subcommittee or senior management in approving the due diligence assessment and outsourcing agreement;

e) Establish procedures for monitoring performance under the outsourcing agreement continuingly; and

f) Address the renewal process for outsourcing agreements and how the renewal will be conducted.

13.4 Additional requirements for the due diligence of cloud computing arrangements are set out in Annexure A.

14. Outsourcing contract

14.1 The outsourcing arrangement between a banking institution and a third party service provider must be governed by a written contractual agreement and must be supported by Service Level Agreements. These contracts are required for all outsourced activities or functions, including insourced and cloud computing activities and must be directly between the banking institution and the third party service provider.

14.2 The outsourcing contract must be between the banking institution and the third party service provider. Where a parent company has concluded an agreement with a third party service provider, which includes the banking institution, the banking institution must be a signatory to this contract with the third party service provider if the banking institution benefits from the services provided.

14.3 The contract should stipulate the rights and responsibilities of both parties pertaining to the following aspects:

a) Audit and monitoring procedures;

[1] Vendor concentration and systemic risk refers to instances where the industry has significant exposure to a particular third-party service provider manifesting as lack of control of individual banking institutions over the service provider or systemic risk to the industry as a whole.

b) Business disruption and contingency plan;

c) Commencement and end dates;

d) Confidentiality, integrity, privacy and security of information including data loss and breach notifications;

e) Customer complaints and dispute resolution arrangements;

f) Default arrangements, termination provisions and operational continuity in the event of bank resolution;

g) Establishment and monitoring of performance levels and standards;

h) Fee methodology and fee disclosure;

i) The geographical location of data, offshoring arrangements and foreign legal requirements;

j) Domestic banking institution skills or capacity constraints and skills transfer;

k) Indemnification, limits and liability;

l) Insurance cover;

m) Notification of business disruption, financial difficulty, catastrophic events and significant incidents;

n) Provisions for amendment and periodic review;

o) Remedies (including early-exit options and penalties) for non-performance;

p) Reporting requirements;

q) Responsibility for providing, receiving, and retaining information;

r) Responsibility for compliance with applicable laws and regulations;

s) Rights of regulatory and supervisory authorities, including unrestricted access to information and right to audit;

t) Roles, rights and responsibilities of the parties;

u) Scope and nature of the arrangement and services to be supplied; and

v) Subcontracting.

14.4 The contractual agreement must detail the pricing methodology and considerations for any fees charged for outsourced activities or functions, including insourcing. A detailed and comprehensively granular invoice must be provided to each banking institution justifying the fees charged.

14.5 The outsourcing contract must contain an indemnity clause to the effect that any sub-contracting by a third-party service provider of the outsourced activity or function is the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor. The banking institution is required to notify the Bank in writing of the augmentation of an existing outsourcing arrangement to include subcontracting of material activities or functions.

14.6 A banking institution should ensure that the outsourcing contract does not entitle the service provider to unilaterally cancel the agreement in the event that a recovery or resolution action is taken by the Bank.

14.7 The terms of the contractual agreement should allow a banking institution to modify the manner in which the outsourced activities or functions, including cloud computing, are performed, specifically where banking institutions may need to amend processes to meet the compliance requirements.

14.8 Where a banking institution makes use of a third party in the use of outsourcing, including cloud computing, the banking institution should ensure that it contractually agrees on the compliance requirements with the service provider to ensure ongoing compliance with laws and regulations where the data shall be hosted.

14.9 Additional requirements for the contractual agreements for cloud computing is set out in Annexure B.

15. Managing and monitoring outsourcing relationship

15.1 A banking institution should ensure that sufficient and appropriate resources are available to manage and monitor the outsourcing relationship. The type and extent of resources required will depend on the materiality of the outsourced business activity or function. Personnel with oversight and management responsibilities for service providers should have an appropriate level of expertise to manage the outsourcing arrangement and must be duly appointed to this role. Monitoring should be ongoing for the duration of the outsourcing relationship and should be an essential component of the banking institution's risk management process.

15.2 Monitoring of outsourced activities and function should, at a minimum, include the following:

a) Verifying that the integrity of the systems and controls of the third party service provider are maintained.

b) Identification of any problems, including financial concerns, encountered by a third party service provider.

c) Maintaining appropriate levels of regular contact with the third party service provider, ranging from daily operational contact to senior management involvement.

d) Regular monitoring of service levels and performance under the agreement.

e) Escalation of issues, e.g., non-performance or breach, identified to the relevant structures of the banking institution.

15.3 A banking institution should ensure that processes are in place to identify and deal with any weaknesses in a third party service provider's performance that may have an adverse impact on the service provided to the banking institution. A banking institution should ensure that data is not stored in jurisdictions that may inhibit effective access to data for the Bank. In considering jurisdictions, a banking institution should continually take into account the political stability and security of the jurisdiction as well as the legislative requirements of the jurisdiction in question. This should include consideration of the legal enforcement provisions within a jurisdiction.

15.4 A banking institution's internal auditor should review the banking institution's material outsourced business activities or functions and ensure that they are in line with the outsourcing policy and should report the findings to the board audit committee.

15.5 The Bank may request a banking institution's external auditor, or an appropriate external expert, to provide an assessment of the risk management processes in place with respect to an arrangement to outsource a material business activity or function. Such assessment should cover areas such as IT systems, data security, internal control frameworks and business continuity plans. The cost of the assessment report should be paid by the banking institution. The report should be made available to the Bank as and when required.

16. Contingency planning and business continuity

16.1 A banking institution should develop contingency plans to ensure business and operational continuity in the event that a third party service provider fails to perform the business activity or function.

16.2 Contingency plans relating to the outsourced activity or function should be reviewed regularly in line with the banking institution's policy, the Determination on Information Security (BID-30) and other relevant legislation with specific consideration of operational continuity in the event of vendor failure or institutional failure.

16.3 In the process of developing contingency plans, a banking institution should, as a minimum, do the following:

a) Consider availability of alternative third party service providers in the event that the arrangement with the outsourcing service provider is unexpectedly terminated and ensure the legal ability for contractual transfer should the need arise.

b) Determine the procedures that need to be in place to ensure minimum disruption to a business when an alternative third party service provider is sought.

c) Ensure that the banking institution has records necessary to sustain business operations and meet its statutory obligations.

d) Ensure that a disaster recovery and business continuity plan is in place for the outsourced activity or function.

e) Assess the adequacy and effectiveness of a third party service provider's disaster recovery and business continuity plans.

f) Periodically obtain evidence of testing that the third party service provider's business continuity and contingency plans are adequate and effective.

g) Maintain an exit strategy, including a pool of comparable third-party service providers, if a contracted third party service provider is unable to perform, and test such exit strategy periodically.

h) Ensure data can be returned or migrated timely to another service provider in a machine-readable format.

17. Supervisory access to information

17.1 A banking institution should provide the Bank with access to necessary information on the outsourced material business activity or function to enable the Bank to exercise its regulatory responsibilities.

17.2 A banking institution should inform the Bank of any possible restriction on the provision of information relating to the outsourced activity or function.

17.3 In order to facilitate the ability to regulate and access a banking institution's data, each banking institution must ensure that:

a) The contractual agreement must include the right of supervisory institutions to access information, which may include conducting on-site visits at the third party service provider's facilities, where necessary.

b) Should the senior management of a banking institution become aware of any possible restriction on the access to regulatory data, the Bank has to be informed as soon as practically possible.

c) The contractual agreement should provide for the mutual exchange of information (potentially through a right to transparency clause) and, by request, the provision of relevant information to the Bank. Where a banking institution is unable to present data to the Bank upon request, for any reason whatsoever, the Bank will require the outsourcing arrangement be brought into compliance with this Determination and may request the termination of the relationship with the third party service provider and take further steps as deemed necessary.

18. Documentation and reporting

18.1 A banking institution should document and report on its outsourcing risk management processes.

18.2 The documentation and reporting should facilitate the accountability, monitoring, and risk management associated with third party service providers to both the banking institution's board of directors and senior management and should include the following:

a) An up-to-date inventory of all outsourcing relationships.

b) Due diligence results, findings, and recommendations.

c) Analysis of costs associated with each outsourcing arrangement, including any direct costs incurred by a banking institution.

d) Executed contracts.

e) Regular risk management and performance reports required and received from the service provider.

f) Regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of service providers performing material business activities or functions.

g) Regular reports to the board and senior management on the results of independent reviews on the banking institution's overall risk management process.

18.3 A banking institution must comply with the reporting and submission requirements set out in this Determination. Each banking institution is required to submit to the Bank on an annual basis, by no later than 31 March each year, a statutory return on all material outsourced activities, including cloud computing relationships held as of 31 December of the preceding year.

PART VI: EFFECTIVE DATE

18. Effective Date

This Determination comes into effect on the date of the publication in the Government Gazette.

Any existing outsourced or cloud computing arrangements must be brought into compliance with this Determination within one year of the publication of this Determination.

Questions relating to this Determination should be addressed to the Director, Banking Supervision Department, Bank of Namibia, Tel: 283 5040.

ANNEXURE A

Additional requirements for the outsourcing of services relating to cloud computing.

The due diligence conducted before the implementation of a cloud computing outsourced arrangement should include assessments under the following headings:

1. Business Case

1.1. A banking institution should have a valid and documented business case for moving each IT service to cloud computing. The business case should identify the link between cloud computing and how it supports the business strategy of the banking institution.

1.2. The business case should clearly define the expected benefits from the arrangement and how these are to be measured.

1.3. The business case should contain a cost versus benefit analysis.

1.4. The business case should indicate how the banking institution's data strategy is addressed, in terms of the classification of data and data residence.

2. Stakeholders

2.1. Input should be obtained from all relevant stakeholders to ensure strategic alignment within the banking institution, e.g., with the IT, IS or Risk Departments.

2.2. The banking institution should identify all relevant stakeholders who may include, further to the above examples, compliance, finance, internal audit and legal functions, which should provide input into or have an insight into the business case.

2.3. A banking institution should, as part of considering cloud computing initiatives, obtain an understanding of the interdependencies in its enterprise and application architecture.

2.4. A banking institution should involve information security and security architecture subject matter experts in the design of cloud-based solutions.

2.5. A banking institution should consider the impact of cloud computing on its configuration management as well as its IT provisioning processes.

3. Information Security Assessment

3.1. Factors to be considered in assessing the adequacy of information security controls includes:

3.1.1. The materiality of the IT systems.

3.1.2. Nature of the process or activities involved.

3.1.3. The classification of data.

3.1.4. Third parties or subcontractors involved.

3.1.5. The location of data and backups.

3.1.6. The cloud deployment model.

3.1.7. Compliance with the Determination on Information Security (BID-30).

3.2. Risks should be clearly described and at a level of granularity that allows for a meaningful understanding of the actual risk and identification of specific mitigating controls (including any required remediation actions).

3.3. The use of scenario analysis to contemplate plausible security events (including a loss of availability) may be useful in aiding the understanding of the risks involved with the arrangement.

3.4. The strength of the control environment should be appropriate for the risks involved in the arrangement. An understanding of the nature and strength of controls required may be strengthened through initial and periodic assessments (such as after a material change) of the design and operating effectiveness of implemented controls.

4. Information Security Considerations

4.1. A banking institution should obtain assurance from third parties involved and contractually agree that third parties will adhere to the information security requirements defined by the banking institution. The information security requirements should deal with patch management, authentication, authorisation, administration identity and access management.

4.2. A banking institution should agree on data loss and breach processes with any third party involved and ensure they are aligned with the banking institution's risk appetite, legal requirements and regulatory obligations.

4.3. Contractual agreements should clearly define accountability and penalties in cases where controls are breached, including who would be responsible for losses resulting from a data breach.

5. Assurance and Testing

5.1. The contractual agreement with any third party involved should specify how a banking institution will verify adherence to the agreed information security requirements. This may include, but not be limited to, third-party assurance audits as well as any other security testing requirements such as vulnerability scanning and penetration testing.

5.2. A banking institution should obtain a copy of any third party's information security policy in order to determine whether it contains adequate provisions for security standards and controls, which would be in line with the banking institution's service level agreement (SLA) with the third party.

6. Security Standards

6.1. A banking institution should be aware of the information and security technology governance and control frameworks or standards that any third party involved in cloud computing adheres to. It should further be aware of whether the third party is certified or audited in terms of any of these and should obtain assurance through obtaining copies of audit/assurance reports on adherence.

6.2. A banking institution should consider leading standards and control frameworks provided by reputable institutions such as the National Institute of Standards and Technology (NIST), the Cloud Security Alliance (CSA) and the Information Systems Audit and Control Association (ISACA).

6.3. Agreed security requirements should include physical security standards at the third party's data centres, which should not be less than the physical security measures that would have been in place had the data been hosted at the banking institution's own data centres.

7. Access Rights

7.1. Access rights to information assets in the cloud or offshored data should be restricted in line with the banking institution's user access management policies which, for instance, include administrator access to operating systems as well as databases.

7.2. Third parties involved in either cloud computing arrangements should develop and implement adequate user access privilege controls in order to restrict access to the banking institution's data, systems and infrastructure. This should be done in a granular fashion and on a least-privilege basis. It remains the responsibility of the banking institution to ensure that these controls are in place and are operating efficiently.

7.3. The banking institution remains responsible for ensuring that processes for user on-boarding, termination and job function changes are managed in a timely and controlled manner in line with its user access policies.

8. Encryption

8.1. A banking institution should determine the level of encryption required in line with the classification of the data involved in the cloud computing arrangement. With cloud computing, the deployment model followed is also of relevance in determining the appropriate level of encryption. All subsequent encryption considerations should be read in line with the principle that the level of the encryption should be commensurate with the materiality of the data and risks involved.

8.2. A banking institution would use different classifications, but for any personal, private or confidential data in a multitenant or community cloud environment, the banking institution should consider encrypting data in transit and at rest.

8.3. Where encryption is required, data should be encrypted before it is moved to the cloud and the same level of encryption services should be used or data at rest and in motion.

8.4. Access to encryption keys should be restricted in line with the banking institution's key management policies and procedures. Where third parties are involved, key management should be subject to the same level of control as outlined in the banking institution's policies and procedures.

8.5. Policies and procedures should cover public key infrastructure, cryptographic protocol design and algorithms used, access controls in place or secure key generation, recoverability, exchange and storage, where applicable.

8.6. Where third parties are used, they should inform the banking institution and the Bank of changes within their cryptosystems.

9. Incident Management

9.1. The contractual agreement with any third party involved in cloud computing should refer to the incident management process between the parties and sets out the roles and responsibilities of the respective parties.

9.2. The incident management process should include incident notifications, responses, remediation, documentation, timelines, addressing the risk of the incident, escalation, and formally closing incidents.

9.3. The contractual agreement with the third party should define the types of incidents (for instance, data breaches and security violations), events and the actions to be initiated after each type of incident.

9.4. A banking institution should be informed when their data may have been seized or accessed by a foreign country, even if it is through appropriate legal processes in that country. The banking institution must, in turn, inform the Bank of such an occurrence.

10. Multitenancy in the Cloud

10.1. It is the responsibility of a banking institution to ensure that its security requirements are commensurate with its risk appetite. The banking institution should take reasonable steps to ensure that its data is sufficiently protected, irrespective of whether it is hosted on-premises or in the cloud.

10.2. As part of defining and agreeing to security standards, the security configuration baseline to prevent cross-contamination with other customer environments should be considered.

11. Forensic Audits and Investigations

11.1. Forensic measures for public data hosted on a public cloud should be commensurate with a banking institution's risk appetite. It is expected that the control measures in the cloud environments should be commensurate with the internal controls of the banking institution and that sensitive data should not be subjected to less stringent control measures in a cloud or offshored environment.

11.2. Data produced for regulatory reporting purposes should be reconcilable with source data, and a banking institution should be able to prove that the integrity of such data has been persevered, which includes data reported to all regulatory authorities.

11.3. Where a forensic audit is not available to a banking institution, it should consider whether the risk is justified for each cloud initiative, particularly considering the sensitivity of data involved and compliance requirements.

11.4. A banking institution should consider the availability of data and records if required for forensic audits, which may, specifically in a multitenant environment, be comingled and migrated among multiple servers located across national boundaries, which may make it impossible to identify specific data.

11.5. A banking institution should consider that where a court, foreign regulator, experts acting on behalf of a foreign regulator or government grants access to a third party's servers, such local authorities might have access to the banking institution's forensic data. This should ideally not include the banking institution's customer data, which should be encrypted, with the banking institution restricting access to the encryption keys.

12. Contingency Planning and Capacity

12.1. Before entering into a contract with a third party, a banking institution should assess whether the third party has sufficient capacity to effectively manage, on a continuous basis, the services that the banking institution is planning to move to the cloud. The banking institution should also consider the potential increased services that the third party may have to provide in the foreseeable future, including the relevant metrics, for capacities, such as storage capacity, bandwidth requirements, increased number of users, and transactions per second requirements.

12.2. Before entering into any third-party contracts, the banking institution should consider whether the information communications infrastructure between the banking institution and the third party is sufficient to manage the current and future requirements on a continual basis.

13. Continuity and Recoverability

13.1. A banking institution should be able to recover from any failure of a third party within a reasonable timeframe as well as within legal and regulatory imposed timelines.

13.2. Business continuity requirements, such as recovery time and recovery point objectives (RTOs and RPOs), should be identified through a business impact assessment, documented, and, where third parties are involved, agreed with third parties.

13.3. Disaster recovery and business continuity plans should be developed to maintain continuity of the banking institution's operations, including matters related to the recovery from an incident, plans for communicating incidents, and the frequency of testing the adequacy and effectiveness of these plans.

13.4. Resilience should be built into the banking institution's cloud computing arrangements.

13.5. Before contracting with any third party, a banking institution should consider whether the third party's business continuity measures are commensurate with the banking institution's requirements.

13.6. A banking institution should have access to the audit or assurance reports of a third party's business continuity programme, including disaster recovery testing, process audits and control audits, at least for activities or functions manage on their behalf.

13.7. The third party's business continuity programme should ideally be certified or mapped to internationally recognised standards, such as ISO 22301 (business continuity management systems).

13.8. The roles and responsibilities of the banking institution and any third party in the event of disruption should be clearly defined in the contractual arrangements.

13.9. A banking institution retains overall responsibility to ensure the availability of its data and services to persons/entities that may legally access such data and services.

13.10. Contingency plans pertaining to outsourced activities should be reviewed regularly but not less than once a year.

ANNEXURE B

Additional requirements for the comprehensive contractual agreement, including Service Level Agreements (SLAs) for cloud computing outsourced services.

1. General

1.1. The contract, which may or may not include the agreed upon service levels, and SLAs should be reviewed by a banking institution's legal counsel before being signed, and the cloud computing relationship should not start before the contract has been signed by all parties.

1.2. The contractual agreement with the third parties involved in cloud computing should define the third party's contractual obligation as guardian of a bank's data.

1.3. Banks should ensure that the contractual agreement provides all elements relevant to the cloud computing arrangement, including sufficient protection of data applicable to the nature of services being offered, deployment of services structurally and geographically, and compliance with the laws in the various jurisdictions where the data will be hosted or stored.

2. Data Ownership

2.1. The contractual agreement with any third party involved in cloud computing arrangements should clearly state that the banking institution retains ownership rights of the data.

2.2. Both the banking institution and the third party should understand how the data ownership rights are affected by the different laws of the countries which will host the data.

2.3. A banking institution should obtain assurance from the service provider of cloud computing that data, including all copies and backups, are stored only in geographic locations permitted by the contractual agreements in line with the banking institution's regulatory and legislative compliance requirements.

2.4. The contractual agreement should clearly state which activities may be subcontracted by a third party and that such arrangements would be subject to full compliance with the primary contractual agreement, including meeting all regulatory and compliance requirements stipulated therein. The primary contract should clearly state that the service provider remains liable for performance in terms of the contract despite any subcontracting arrangements.

2.5. The service provider shall provide an undertaking to treat the banking institution's data with the utmost confidentiality at all times and to ensure that its employees and service providers adhere to the same standard of confidentiality. Access should be restricted on a least privileged basis.

3. Data Breaches

3.1. A banking institution is responsible for ensuring that the contractual agreement with the service provider ensures that it is able to meet its data breach notification or other legal reporting requirements.

3.2. The contractual agreement should define roles and responsibilities in case of a data breach, including cooperative processes to be implemented during the investigation and any follow-up actions.

3.3. The contractual agreement should define the penalties payable by the third party for data breaches where the third party did not adhere to the terms of the agreement or was negligent in any other way.

3.4. The use of cloud computing should not inhibit the banking institution's ability to meet its data retention legal requirement.

3.5. All legal documents should be maintained in accordance with the banking institution's legal document management procedures and in accordance with legislative requirements.

4. Termination

4.1. A banking institution must ensure that its intellectual property rights and contractual rights to data are not compromised, despite any cloud computing arrangements which may be in place. Data must always be in a usable, readable and portable state even after the contract is terminated.

5. Planning for Termination

5.1. A banking institution should document the hardware, software and procedural requirements for moving from an existing service provider to another service provider or in-house. As far as it is feasibly possible, the banking institution should avoid being locked into one specific service provider.

5.2. A banking institution needs to ensure that an exit from the cloud computing arrangement does not affect its compliance with any legislative requirements.

6. Contractual Agreements

6.1. Default and termination provisions should be included in outsourcing contracts.

6.2. The contractual agreement should stipulate the roles and responsibilities for both parties at the termination of the agreement, including the circumstances when a banking institution enters into a resolution.

6.3. The contractual agreement should define the manner in which the agreement is to be terminated as well as the guarantees provided to enable the banking institution to resume the performance of the outsourced or offshored activities or to transfer those activities to another service provider upon the termination of the agreement.

6.4. The contractual agreement should include a clause to the effect that, upon the termination of the contract, a banking institution's data be promptly and completely removed and returned to the banking institution, transferred to another service provider or destroyed, depending on the nature of the data involved. The contractual arrangements should include sufficient assurance once its data has been removed, transferred or destroyed at the termination of the agreement.

7. Termination of Services

7.1. Any cloud computing services should be organised in such a way that they do not become a barrier to the resolution or orderly winding-down of a banking institution or create additional complexity in a resolution.

7.2. Where activities, functions or data outsourced are identified in a banking institution‘s recovery plan, the banking institution should provide further detail and guidance in the recovery plan on the cloud computing involved, such as the effect recovery would have on the relationship as well as actions required to ensure continuity during recovery of the banking institution or failure of the service provider.

7.3. The contractual agreement for cloud computing arrangement, specifically any default clause, may not entitle the service provider to unilaterally cancel the agreement in the event that a recovery or resolution action is taken.

8. Interoperability

8.1. A banking institution should consider interoperability before outsourcing activities or functions to a cloud service provider.

8.2. As part of its business continuity planning and testing, a banking institution should maintain as well as test procedures, capabilities and alternatives to transfer cloud computing and operations in-house or to another third party as part of a scenario where the current third-party service is no longer able to meet its contractual obligations.

8.3. The banking institution should have contingency plans in place to continue with its operations in case of an unforeseen event, irrespective of whether a cloud environment had been deployed. The banking institution’s risk management processes should determine the level and extent of contingency plans to be instituted. The operational requirements can be addressed on a case-by-case basis, given the existing circumstances.

9. Forensic Audits and Investigations

9.1. The contractual agreement with the third parties responsible for cloud computing must clearly prescribe the access that a banking institution, regulatory authorities and law enforcement agencies would have in order to conduct forensic audits and investigations.

9.2. The contractual agreement should prescribe the manner in which forensic evidence is made available to the banking institution as well as the controls in place as proof that such evidence has not been compromised.

9.3. The contractual agreement should define the roles and responsibilities of both parties in terms of forensic data. This should, for instance, include who is responsible for logging which data.

9.4. The contractual agreement should also determine which forensic tools are available to a bank directly or via a third party.

9.5. The contractual agreement should further stipulate both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony. A banking institution should be able to provide adequate assurance to investigate, and regulatory authorities that all data requested has been retrieved.

9.6. The contractual agreement should stipulate the duration during which forensic data would be available to a banking institution. The contractual agreement with the third party should require assurance that the banking institution's data is preserved as recorded, which includes both the primary data and secondary information such as metadata and logs.