GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$23.20 WINDHOEK - 26 November 2024 No. 8513

CONTENTS

Page

General Notice

BANK OF NAMIBIA

No. 765 2024

DETERMINATION UNDER THE BANKING INSTITUTIONS ACT, 2023:
CLOUD COMPUTING

In my capacity as Governor of the Bank of Namibia (Bank), and under the powers vested in the Bank in terms of section 108(3)(b) of the Banking Institutions Act, 2023 (Act No. 13 of 2023), I hereby issue the Determination on Cloud Computing (BID-19).

J. !GAWAXAB
GOVERNOR
BANK OF NAMIBIA

Windhoek, 8 November 2024

Arrangement of paragraphs

PART I
PRELIMINARY

PARAGRAPH

PART II
STATEMENT OF POLICY

PART III
IMPLEMENTATION AND SPECIFIC REQUIREMENTS

PART IV
EFFECTIVE DATE

PART I: PRELIMINARY

1. **Short Title** – Cloud Computing

2. **Authorisation** – The authority for the Bank to issue this Determination is provided in terms of section 108(3)(b) of the Banking Institutions Act, 2023 (Act No. 13 of 2023).

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

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

4.1 **"Act"** means the Banking Institutions Act, 2023 (Act No. 13 of 2023).

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 **"Banking Institution"** means a banking institution as defined in the Act.

4.4 **"Cloud-based services" or "cloud computing"** means a set of on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage facilities, applications and services) which can be rapidly provisioned and released with minimal management effort or service provider interaction. Platforms owned or managed by parent/group companies are not considered as cloud-based services or cloud computing.

4.5 **"Cloud Service Model"** means a type of computing resource that is offered by a cloud service provider. There are three main types of cloud service models**:**

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

(b) **"Platform as a Service (PaaS)"** means a complete computer environment 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 a banking institution is provided computing resources, including servers, networking, storage, and data centre space by the cloud service provider. 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.

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

4.6 **"Cloud adoption"** means a process or strategy that provides incentives for banking institutions to use cloud computing for their computing requirements in a way that is efficient and sustainable.

4.7 **"Core banking systems"** means core banking systems as defined in the Act.

4.8 **"Cloud migration"** means a process of moving data, applications, hardware, software, network infrastructure and/or other business elements and services to a cloud computing environment.

4.9 **"Cloud service provider"** means a local or international company that offers a range of cloud computing services, including infrastructure, platforms, and software, over the internet. These services allow organisations to access computing resources such as servers, storage, databases, networking, and software applications on-demand, without a need to invest in and maintain physical hardware or software in-house.

4.10 **"Encryption"** means a process of converting data or information into a code to prevent unauthorised access by human or computer systems.

4.11 **Identity and Access Management** means the cybersecurity discipline that deals with how users access digital resources and what they can do with those resources. Identity and Access Management systems keep hackers out while ensuring that individual users have the exact permission they need to do their jobs.

4.12 **"Latency Levels**" are acceptable time delays for processing and delivering data or services via the cloud, with different latency requirements applicable, based on the criticality of applications and compliance standards. These levels are essential to ensure the performance, reliability, and security of cloud services.

4.13 **"Material Cloud Service**" means:

(a) a service of such importance that any weakness or failure in the provision of this service could have a significant impact on the banking institution or microfinance banking institutions ability to meet its regulatory responsibilities, to continue in business, or cause a significant disruption in the business operations of the banking institution or microfinance banking institution. A significant impact is an event that causes the banking institution not to meet Regulatory requirements around Recovery Time Objective and Recovery Point Objective; or

(b) a service which involves customer information or other sensitive information, and which in the event of any unauthorised access or disclosure, loss or theft may have a material impact on the banking institution or its customers; or

(c) a service involving core banking systems and/or services; or

(d) any other service which meets the materiality criteria as approved by the board of a banking institution or microfinance banking institution. The banking institution or microfinance banking institution must develop materiality criteria and metrics on how to define and measure the materiality of the impact of an event based on the "threshold" table provided in the Circular on the Determination on Information Security: BIA 1/30 that allows the banking institution's to measure its compliance to Regulatory set Recovery Time Objectives and Recovery Point Objectives.

4.14 **"On-premises"** means computer systems that are located within the physical confines of the banking institution or microfinance banking institution.

4.15 **"Outsourcing"** has the same meaning as provided in the Determination on Outsourcing (BID-34).

4.16 **"Outsourcing arrangement"** has the same meaning as provided in the Determination on Outsourcing (BID-34).

4.17 "**Phased**" refers to a gradual or step-by-step implementation approach. This means that cloud adoption is carried out in distinct stages or phases, rather than all at once. Each phase or stage often involves specific milestones, objectives, or components being transitioned to the cloud, allowing for controlled, manageable progress and ensuring that risks are assessed and mitigated at each stage.

4.18 **"Third-party service provider"** means an entity that is undertaking the outsourced function or activity on behalf of the banking institution or microfinance 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.

4.19 **"Vendor Lock-in"** means a situation in which the banking institution or microfinance banking institution using the cloud product or service of a cloud service provider cannot easily transition to a competitor's cloud product or service.

4.20 **"Virtualization"** means the concepts and technologies that allow for the creation of a virtual version of a device or resource, such as a server, storage device, network or operating system through a framework that divides the resource into one or more execution environments.

PART II: STATEMENT OF POLICY

5. Purpose

5.1 This Determination sets out the requirements that a banking institution or microfinance banking institution must observe in assessing and managing risks relating to cloud computing arrangements to establish a comprehensive framework for the secure, compliant and effective use of cloud computing services by banking institutions.

5.2 This Determination aims to ensure that cloud environments are resilient against cyber threats, compliant with regulatory requirements and capable of driving innovation and operational efficiency. By setting principles for risk management, data protection and service oversight, this Determination seeks to foster transparency, accountability and continuous improvement in the adoption and management of cloud technologies within the banking sector.

6. Scope

This Determination guides all aspects relating to cloud computing arrangements of a banking institution or microfinance banking institution.

PART III: IMPLEMENTATION AND SPECIFIC REQUIREMENTS

7. Responsibility

7.1 The Board of Directors of a banking institution or microfinance banking institution is responsible for ensuring compliance with this Determination by:

(a) Developing and enforcing comprehensive cloud governance policies that define roles, responsibilities, and procedures for managing cloud services. These policies should cover areas such as data security, cyber security, access management, compliance, and incident response.

(b) Ensure that associated risks are duly identified, understood, monitored and mitigated.

(c) Approving the criteria to assess the materiality of the cloud services.

(d) Implementing a risk management framework to identify, assess, and mitigate risks associated with cloud services.

(e) Approving and overseeing material cloud services and ensuring that there is an appropriate business continuity and contingency and exit plan for such services.

(f) Ensuring that it is duly apprised of all cloud services at the outset and on an ongoing basis and that it is promptly informed of any critical issue and incident.

(g) Ensuring that there is an appropriate risk assessment framework and adequate oversight and coverage by the control functions and the external auditors.

(h) Ensuring that the Board, Senior Management and other relevant staff have an adequate level of expertise and experience and are provided with the relevant training for effective oversight of the cloud services.

(i) Ensuring cloud service providers adhere to data protection laws and regulations, including data encryption, data residency requirements, and privacy standards. Cloud service providers must implement measures to prevent unauthorized access, data breaches, and data loss.

(j) Ensuring that the Bank and the microfinance banking institution or microfinance banking institution's external auditors have immediate access to information relating to the cloud computing arrangement to enable them to execute their duties under the Act and other relevant legislation.

7.2 Branches and subsidiaries of foreign banking institutions may adopt the cloud strategy and policy on the use of cloud services of their parent companies, provided that the referred to strategy and policy is in line with the requirements of this Determination. Branches of foreign banking institutions which do not have a local Board must ensure that material cloud services are duly approved by the Board of Directors of their parent bank or the relevant sub-committee or authority as designated by their parent company.

7.3 Senior Management is required to ensure that the following key requirements relating to cloud computing arrangements are in place:

(a) A policy for the use of cloud services is duly documented and approved by the Board.

(b) A plan for assessing cloud computing strategies and arrangements and evaluating their consistency with and supporting the banking institution's strategic objectives is established.

(c) Comprehensive risk assessment and risk mitigation strategies to address the risks associated with cloud migration and cloud computing arrangements with service providers.

(d) Ensure Cloud Service Providers conduct regular audits, vulnerability assessments, and updates to ensure compliance with the latest encryption and security practices as technologies evolve.

(e) Ensuring that the appropriate cloud service model and cloud deployment model are used taking into consideration the materiality of the IT assets involved and the security arrangement in place.

(f) Conduct thorough due diligence on cloud service providers before engaging their services. Assess cloud service providers' security posture, compliance capabilities, and track record. Continuously monitor Cloud service providers for changes in risk profile, compliance status and security incidents.

(g) Ensure that there is a clear delineation of the responsibility and accountability between the banking institution and the cloud service provider, that the responsibilities resting on the banking institution are well understood and managed and that the responsibilities of the cloud service provider are duly managed with appropriate oversight from the banking institution.

(h) Ensure that the Board is kept informed of the implementation status and ongoing performance of cloud services and cloud service providers as well as of any current or emerging risks and issues.

(i) Ensure that there is an ongoing monitoring of the performance of the cloud services and the cloud service providers and timely identification, escalation and reporting of incidents.

(j) Seek approval from the Bank before entering cloud computing arrangements regarding the outsourcing of material functions and activities as required and outlined in the Determination on Outsourcing (BID-34).

7.4 A banking institution or microfinance banking institution remains accountable for compliance with all legislative requirements and must ensure that a contractual agreement with cloud service providers incorporates the necessary arrangements that will enable them to remain compliant by performing periodic reviews, at least on an annual basis, of contractual agreements to ensure these remain aligned with evolving regulatory requirements and best practices.

8. Cloud Consideration

8.1 A banking institution or microfinance banking institution must apply to the Bank to seek approval for the phased deployment of material cloud services or core banking systems.

8.2 The application must be done at least sixty (60) days before the proposed deployment of the cloud services to allow the Bank to assess the application. The application must be accompanied by an attestation from the Chief Executive Officer or Managing Director of the banking institution as well as an internal audit verification confirming, inter alia, the approval of the board and compliance with this Determination, by submitting to the Bank the completed Schedule I and II of the Annexure as well as compliance with the following requirements:

(a) A comprehensive risk-based board-approved policy on cloud services, either on a stand-alone basis or integrated within relevant existing policies and which policy must take into consideration the requirements outlined in this Determination. The policy must be aligned to the overall information technology cloud strategy and risk appetite of the banking institution and reviewed at least on an annual basis or at such higher frequency as may be specified, or subsequent to material events which can be determined by the

Bank based on the "Thresholds" table as provided in the Circular on the Determination on Information Security (BID-30).

(b) Risk assessment report and the ongoing management thereof, including the information security risk assessment, and requirements to ensure there is no undue concentration on single cloud service providers or geographical locations for material cloud services, which can create an over-reliance on a single cloud service provider or geographical location for critical or material cloud services, and which can significantly increase operational, financial, and cyber risks. This risk arises when a failure, outage, or disruption in the Cloud Service Provider or region hosting the cloud infrastructure could cause widespread service disruptions or data loss, with potentially severe consequences for the organisation.

(c) Evaluation of the sufficiency of the current cyber and technology risk management framework and assess whether the skills and knowledge of internal staff (including ongoing training needs) are adequate for effective cloud adoption, deployment and oversight of cloud services. Sufficiency of skills, knowledge, and capacity for cloud deployment should be determined through a combination of certifications, hands-on experience, cloud governance frameworks, technical assessments, and external audits. Banking institutions or microfinance banking institutions must ensure that their teams are adequately trained, capacitated, supported, and capable of managing the unique challenges posed by cloud services.

(d) Demonstrate the ability of the banking institution or microfinance banking institution to effectively manage risks around migrating core banking systems to Cloud Service Providers by providing the Bank with their board-approved cloud strategy**.**

8.3 A banking institution or microfinance banking institution must determine the necessary security controls to be established in line with their risk appetite and consider, among others, the materiality of the cloud service, the criticality and sensitivity of the information and other IT assets involved, the nature of the service, the classification of data, the location of data, the cloud deployment model, virtualization, and cloud service model.

8.4 A banking institution or microfinance banking institution must provide results of the latest Disaster Recovery test as part of the notification, which includes Internal Audit verification and certification that the banking institution is able to run business-as-usual operations for at least 1 week, from its Disaster Recovery Site.

8.5 A banking institution or microfinance banking institution must ensure that there is sufficient redundancy on international links. This is to ensure adherence to Recovery Time Objective requirements, to determine its level of redundancy, that these are within the risk appetite of the banking institution or microfinance banking institution and will allow the banking institution or microfinance banking institution to meet regulatory expectations regarding uptime and availability requirements.

8.6 A banking institution or microfinance banking institution must ensure that cloud service providers meet the requirements set out in Appendix A.

9. Risk Management

9.1 A banking institution or microfinance banking institution must establish a documented risk management framework, clearly articulating how it plans to effectively identify,

assess and mitigate risks associated with cloud computing, including third-party risks and potential data breaches as well as aspects relating to disaster recovery and business continuity, regular penetration testing, employee skills and training requirements, as well as security measures and controls, including, but not limited to, security measures such as identity and access management, catering to both provisioning and terminating roles.

9.2 A banking institution or microfinance banking institution must have in place a cloud computing policy that comprehensively guides the risk management of cloud computing arrangements for material and core banking systems and services. The following aspects must be included in the policy:

(a) Data security and privacy requirements as set out in the Determination on Information Security (BID-30).

(b) Data residency and sovereignty. The policy must require a banking institution or microfinance banking institution to ensure compliance with local laws and data protection standards and alignment with global standards for data residency including guidelines that accommodate both local and multinational compliance frameworks, such as General Data Protection Regulations and cross-border data sharing rules regarding data residency and sovereignty. Cloud Service Provider infrastructure can only be in countries with strong data protection regulations with requirements of prior approval to be obtained from the Bank for data movement outside of those jurisdictions with an exit clause in the agreement in the event of such a breach.

(c) User Data Handling - Implement clear policies for data handling, including processes for obtaining user consent, managing data transfers, and ensuring data integrity during transitions between cloud providers. The policy must require a banking institution to obtain user consent and manage data processing agreements; establish rules for the processing, destruction, and restoration of customer data; and ensure customers can retrieve their data if the cloud contract is terminated.

(d) Cloud Service Provider Liability. Limit Cloud Service Provider's' ability to exclude liability for data loss, service degradation, or data breaches.

10. Materiality Assessment

A banking institution **or** microfinance banking institution must, as a minimum, consider the following factors in their assessment of materiality:

(a) The nature (including the criticality) of the services and the IT assets;

(b) The potential direct and indirect impact that a confidentiality breach failure or disruption of the services could have on the banking institution and its customers. This includes the ability of the banking institution to meet its legal and regulatory requirements to continue its business operations and provide its services;

(c) The value chains of key processes should be assessed such as those enabling core banking functions for instance payments, transfers, savings, and investments;

(d) The degree of difficulty in finding or migrating to an alternative cloud service provider or to bring the services in-house;

(e) The potential impact of the service on current and projected earnings, solvency, liquidity, funding capital and risk profile;

(f) The ability to maintain appropriate internal controls and meet regulatory requirements in case of operational failures by the cloud service provider; and

(g) Any other matter as the Bank may determine.

11. Compliance and Auditing

11.1 The Bank requires cloud computing arrangements of a or banking institution microfinance banking institution to be prudently and comprehensively managed in a manner similar to any other vendor. The cloud computing arrangement must be set at arm's length and must not impair the banking institution or microfinance banking institution's ability to comply with regulatory requirements. Fees levied must be documented, transparent and commensurate with services rendered.

11.2 A banking institution or microfinance banking institution must not engage in a cloud service without entering into a written agreement with the cloud service provider. The written agreement must contain appropriate clauses on access to information stored on the cloud by the banking institution and the Bank. For subsidiaries and branches of foreign banking institutions, the agreement may comprise a master agreement entered by the respective foreign banking institution with a relevant addendum for the local entity. The agreement must ensure forensic audits and investigations by Law Enforcement and obligations by banking institutions and cloud service providers when investigations occur.

11.3 Adoption of Standards:

(a) Cloud service providers contracted by banking institutions or microfinance banking institutions are required to achieve and maintain the latest ISO 27001 certification or any latest ISO certification standards pertaining thereto, demonstrating a commitment to establishing, implementing, maintaining, and continuously improving an information security management system. This includes policies for risk assessment, risk treatment, and security controls.

(b) Cloud service providers contracted by banking institutions must ensure the adoption of other relevant standards such as ISO 27017 (cloud security), ISO 27018 (protection of personal data in the cloud), NIST SP 800-53 (security and privacy controls), and Payment Card Industry Data Security Standard(for payment card data security), as well as use of the latest versions of such standards.

(c) Cloud service providers contracted by banking institutions must undergo annual audits to maintain compliance with amongst others international standards, ensuring that security measures, risk management protocols, and data protection controls remain up to date.

11.4 Reporting and Verification:

A banking institution or microfinance banking institution is required to provide a compliance report of its cloud service provider at least on an annual basis, or on a more regular frequency as may be specified by the Bank, demonstrating their adherence to the required standards. This report should include audit results, remediation actions, and any changes in compliance status.

11.5 A banking institution or microfinance banking institution must ensure that, as a minimum, third-party audits are conducted at least annually on the cloud service providers to ensure adherence to security and compliance standards.

11.6 Requirements for Maintaining Audit Logs and Security Incident Reports for Systems Hosted on the Cloud.

(a) A banking institution or microfinance banking institution must ensure the collection and retention of comprehensive audit logs for all critical cloud activities, including user access, configuration changes, data transfers, and security events. Logs should be retained for a period of 3 years.

(b) A banking institution or microfinance banking institution must ensure that audit logs are tamper-evident and protected against unauthorised access. Logs must be securely stored and encrypted to maintain their integrity and confidentiality.

(c) A banking institution or microfinance banking institution must implement real-time monitoring and analysis of audit logs to promptly detect suspicious activities, security breaches, and policy violations.

11.7 Security Incident Reporting for Systems Hosted on the Cloud.

(a) A banking institution or microfinance banking institution must establish criteria for identifying and classifying security incidents based on their severity, impact, and nature. Incidents should be categorised to prioritise response efforts.

(b) A banking institution or microfinance banking institution must define clear procedures for reporting security incidents as outlined in section 13 – Incident Response and Management.

(c) A banking institution or microfinance banking institution must require detailed documentation of all security incidents, including root cause analysis, remediation steps, and lessons learned.

12. Service Level Agreements

12.1 A banking institution or microfinance banking institution must have detailed Service Level Agreements with cloud service providers, including uptime guarantees, performance metrics, and penalties for non-compliance. The banking institution or microfinance banking institution must also ensure that cloud service providers meet the requirements set out in this Determination, Appendix B, the Determination on Outsourcing (BID-34), and the Determination on Information Security (BID-30) as follows:

(a) Setting expectations for data transfer rates, including minimum throughput levels and guaranteed bandwidth. This can be crucial for services that require high data transfer capabilities.

(b) Establishing acceptable latency levels for various operations, thereby ensuring that the service performs efficiently and meets user expectations.

(c) Defining acceptable error rates for various operations, including thresholds for failed requests or transactions.

12.2 Penalties for non-compliance

(a) Implementation of tiered penalties based on the severity and frequency of Service Level Agreement breaches such as higher penalties for repeated or significant violations.

(b) The right for the banking institution or microfinance banking institution to terminate the contract without penalty if the cloud service providers consistently fail to meet Service Level Agreement requirements over a specified period.

12.3 Procedures for monitoring and reporting Service Level Agreement compliance

(a) A banking institution or microfinance banking institution must use automated monitoring tools to continuously track performance metrics and uptime. These tools should provide real-time visibility into the cloud service providers' performance against Service Level Agreement commitments.

(b) A banking institution or microfinance banking institution must define the frequency of monitoring activities, thereby ensuring that it is frequent enough to detect Service Level Agreement breaches promptly. This may include continuous monitoring or periodic (e.g., hourly, daily) checks.

(c) A banking institution or microfinance banking institution must specify the types of data to be collected for monitoring purposes, such as logs, performance metrics, and system health indicators. The banking institution or microfinance banking institution must further ensure data integrity and security during collection and storage.

12.4 Service Level Agreement compliance reporting

(a) A banking institution or microfinance banking must ensure that cloud service providers are required to provide regular compliance reports (e.g., monthly, or quarterly). These reports should detail performance against each Service Level Agreement metric, including any incidents of non-compliance.

(b) A banking institution or microfinance banking institution must ensure that the compliance reports include key information such as uptime percentages, response times, latency, error rates, and any service disruptions. The compliance reports must also include explanations for any Service Level Agreement breaches and the actions taken to address them.

(c) A banking institution or microfinance banking institution must have access to an online portal or dashboard where it can view real-time performance data and historical compliance reports. This increases transparency and

allows a banking institution to monitor Service Level Agreement adherence independently.

12.5 Dispute resolution and exit strategy

(a) A banking institution or microfinance banking institution must ensure that there is a clear process for resolving disputes related to Service Level Agreement compliance which includes steps for raising a dispute, timelines for resolution, and the roles and responsibilities of both the Cloud Service Provider and the customer.

(b) In cases of significant disputes, the banking institution or microfinance banking institution must ensure independent audits by third-party experts to verify Service Level Agreement compliance. The parameters on how the results of such audits will be used to resolve the dispute should be clearly defined.

(c) A banking institution or microfinance banking institution must have an exit clause included as part of the Service Level Agreement to ensure a smooth, secure, and efficient transition when terminating or migrating cloud services. This is crucial for mitigating risks, maintaining business continuity, and safeguarding data integrity. The banking institution or microfinance banking institution must also consider the cost implications and the potential for vendor lock-in that could arise from expensive transitions.

(d) A banking institution or microfinance banking institution must ensure comprehensive and well documented exit strategies and plans are established and reviewed regularly to confirm that they remain adequate and effective. The exit strategy and plan must, as a minimum, include the following:

(i) Agreed process and procedures including reasonable timeframe for deletion by the cloud service provider of all data (bank and customer data) of the banking institution;
(ii) Assurance from the cloud service provider through relevant independent reports and certificates that all data of the banking institution or microfinance banking institution including any backup, is rendered permanently irrecoverable and inaccessible, in a timely manner after termination of the contract;
(iii) Transferability of services (to a third party or back to the banking institution) for continuity of service; and
(iv) Identification of alternative solutions to allow for business continuity throughout and after the transition phase.

12.6 Data portability and interoperability

(a) A banking institution or microfinance banking institution must define portability standards that clearly outline data portability requirements to be met by cloud service providers. The portability requirements must enable a banking institution or microfinance banking institution to transfer its data seamlessly between different cloud service providers without loss of data integrity or functionality. This includes structured and unstructured data, metadata and configurations.

12.7 Supervisory access to information

(a) A contractual agreement between a banking institution or microfinance banking institution and a cloud service provider must include the right of a banking institution or microfinance banking institution to access information which may include conducting on-site visits at the service provider's facilities, where necessary, as well as the right of audit (including remote audit) by the Bank, the banking institution or microfinance banking institution, its external auditors, or any third party appointed by the Bank, the banking institution or its external auditors and right of access to relevant audit reports/ reports of other tests conducted by the cloud service provider. The cost of an audit by any third party appointed by the Bank must be borne by the banking institution or microfinance banking institution;

(b) Agreements for material cloud services must also, inter alia, include relevant clauses on the obligation of the cloud service provider to cooperate with the Bank and timeously provide access to information required by the Bank, the banking institution or microfinance banking institution, its external auditors, or any third-party appointed by the Bank.

(c) If a banking institution or microfinance banking institution becomes aware of any possible restriction on access to regulatory data, the banking institution must inform the Bank as soon as practically possible, but not later than forty-eight hours after becoming so aware.

(d) A contractual agreement between a banking institution or microfinance banking institution and a cloud service provider must 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 and ensure that agreements with cloud service providers specify conditions for physical access to data, systems, and infrastructure, particularly for auditing purposes. Public cloud vendors must provide structured reporting for supervisory access.

(e) If a banking institution or microfinance banking institution is unable to provide data to the Bank upon request, for any reason whatsoever, the Bank will require the outsourcing arrangement to be brought into compliance with this Determination and may request the termination of the relationship with the service provider and take further steps as deemed necessary.

13. Incident Response and Management for Systems Hosted on the Cloud

13.1 A banking institution or microfinance banking institution must develop detailed incident response plans, including notification procedures for data breaches.

13.2 Incident response plan development

(a) A banking institution or microfinance banking institution must develop a comprehensive incident response policy that outlines the framework and requirements for handling security incidents. This policy must be aligned with regulatory requirements as outlined in BID-30 and Appendix C.

(b) A banking institution or microfinance banking institution must clearly define the roles and responsibilities of the incident response team (IRT), including team members from IT, security, legal, communications, and other relevant departments.

(c) A banking institution or microfinance banking institution must establish criteria for classifying incidents based on severity, impact, and type (e.g., data breach, malware infection, DDoS attack). This helps to prioritise response efforts and allocate resources effectively. The incident management process should include incident notifications, responses, remediation, documentation, timelines, addressing the risk of the incident, escalation, and formally closing incidents.

(d) The contractual agreement with the cloud service provider 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.

(e) A banking institution or microfinance banking institution must be informed when its 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 or microfinance banking institution must, in turn, inform the Bank within twenty-four hours of such an occurrence.

(f) A banking institution or microfinance banking institution shall immediately, upon becoming aware of IT operational or information security-related incidents as outlined in the Circular on information security (BID 1/30), inform the Director of Banking Supervision Department, through email, telephone or otherwise.

(g) A banking institution or microfinance banking institution must subsequently submit information related to the incident in a return (BIR 301) within 24 hours after detecting the incident or the next immediate working day in case of weekends and public holidays. The banking institution or microfinance banking institution must provide subsequent updates to the Bank on the incidents reported in the return as and when there are changes to the current situation or as requested by the Bank.

(h) A banking institution or microfinance banking institution must submit a full incident report to the Bank for all IT operational and Cyber information security incidents at the end of each calendar quarter, by no later than the 26th day of the following month.

13.3 Stakeholder communication

(a) A banking institution or microfinance banking institution must ensure transparent communications with affected stakeholders, including customers, service providers, and employees, by providing clear and honest information about the incident and its impact. Incident response plans must account for the sensitivity of incidents and the potential for exploitation by malicious actors. Stakeholder communication must be transparent but cautious to prevent further risk.

(b) A banking institution or microfinance banking institution must offer support and resources to affected stakeholders, such as credit monitoring services, identity theft protection, and dedicated hotlines or help desks to address concerns and questions as well as timely assistance to affected customers.

13.4 Establishment of a Disaster Recovery Plan. A banking institution or microfinance banking institution must develop a comprehensive disaster recovery plan that outlines the procedures and processes for restoring IT systems and data within identified and

agreed upon Recovery Time Objectives and Recovery Point Objectives. The plan must cover all critical and/or core systems as well as applications and should be tested on a regular basis, or at a minimum, at least two times per year.

13.5 A banking institution or microfinance banking institution must implement a robust data backup strategy, including regular backups, secure storage of backup data, and periodic testing of backup integrity and must ensure that backups are maintained locally.

13.6 Documentation and review

A banking institution or microfinance banking institution must make use of indepen dent reports to verify that the requirements placed on the Cloud Service Provider are met.

14. Documentation and reporting

14.1 A banking institution or microfinance banking institution must document and report on its cloud computing risk management processes.

14.2 The documentation and reporting must facilitate the accountability, monitoring, and risk management associated with cloud service providers to both the banking institution's Board of Directors and Senior Management and must include the following:

(a) An up-to-date inventory of all cloud service providers.

(b) Due diligence results, findings, and recommendations.

(c) Cost management practices and regular reviews of cloud expenditure through implemented cost management practices to optimise cloud spending, such as resource usage monitoring and cost analysis tools. Analysis of costs associated with each cloud computing arrangement.

(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 cloud service providers.

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

14.3 A banking institution or microfinance banking institution must ensure timely and comprehensive reporting to the Bank on the use of cloud service providers to maintain transparency, accountability, and compliance. Reporting must be made on, but not limited to, the following conditions:

(a) A banking institution or microfinance banking institution must summarise findings from audits and security assessments.

(b) A banking institution or microfinance banking institution must provide details on Service Level Agreements and any breaches thereof.

(c) A banking institution or microfinance banking institution must report on business contuinity and disaster recovery plans and testing results.

(d) A banking institution or microfinance banking institution must report significant changes in cloud services, e.g., changes in cloud service provider, data centre locations, and security protocols to ensure the Bank is informed of any operational or compliance risks.

14.4 A banking institution or microfinance banking institution must comply with the reporting and submission requirements set out in this Determination. Each banking institution or microfinance banking institution **is** required to submit to the Bank on an annual basis, three months after the banking institution or microfinance banking institution's financial year end, a statutory return, confirming compliance with Schedule I for all cloud computing relationships held as of 31 December of the preceding year, as well as the completion of Schedule II for all material and significant changes to the responsibility matrix for all material and core banking system cloud arrangements. The return must be accompanied by Internal Audit verification/certification. The banking institution or microfinance banking institution is required to have an external service provider (not group or parent) perform the attestation or certification on a triennial basis.

PART IV: EFFECTIVE DATE

15. Effective Date

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

16. Repeal of BID-19

This Determination repeals and replaces the Determination on Localisation of Core Banking Systems (BID-19) published as General Notice No. 272 in Government Gazette No. 4109 of 27 August 2008.

Questions relating to this Determination should be addressed to:

The Director
Banking Supervision Department
Bank of Namibia
Tel: 283 5041.

APPENDIX A

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

1. Multitenancy in the Cloud

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

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

2. Forensic Audits and Investigations

2.1 Forensic measures for public data hosted on a public cloud should be commensurate with a banking institution or microfinance 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 or microfinance banking institution and that sensitive data should not be subjected to less stringent control measures in a cloud or offshored environment.

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

2.3 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 the data involved and compliance requirements.

2.4 A banking institution or microfinance 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.

2.5 A banking institution or microfinance banking institution should consider that where a court, foreign regulator, or experts acting on behalf of a foreign regulator or government, grants access to a third party's servers, such authorities may have access to the banking institution or microfinance 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.

3. Contingency Planning and Capacity

3.1 Before entering into a contract with a third party for cloud service provision, a banking institution or microfinance banking institution must assess whether the third party has sufficient capacity to effectively manage, on a continuous basis, the services that the banking institution or microfinance banking institution is planning to move to the cloud. The banking institution or microfinance banking institution must 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.

3.2 Before entering into any third-party cloud service provision contracts, the banking institution or microfinance banking institution must consider whether the information communications infrastructure between the banking institution or microfinance banking institution and the third party is sufficient to manage the current and future requirements on a continual basis.

4. Continuity and Recoverability

4.1 A banking institution or microfinance banking institution must be able to recover from any failure of a cloud service provider within the Regulatory-set Recovery Time Objectives and Recovery Point Objectives.

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

4.3 Disaster recovery and business continuity plans must be developed to maintain the 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.

4.4 Resilience must be built into the banking institution or microfinance banking institution cloud computing arrangements.

4.5 Before contracting with any third party, a banking institution or microfinance banking institution must consider whether the third party's business continuity measures are commensurate with the banking institution or microfinance banking institution requirements and risk appetite.

4.6 A banking institution or microfinance banking institution must 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 managed on their behalf.

4.7 The cloud service providers' business continuity programme must ideally be certified or mapped to internationally recognised standards, such as ISO 22301 (business continuity management systems) and any updates thereto.

4.8 The roles and responsibilities of the banking institution or microfinance banking institution and any third party in the event of disruption must be clearly defined in the contractual arrangements between the contracting parties.

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

4.10 Contingency plans pertaining to outsourced activities must be reviewed regularly by banking institutions or microfinance banking institutions but not less than once a year.

APPENDIX B

Additional requirements for the comprehensive contractual agreement, including Service Level Agreements for cloud computing outsourced services and systems.

1. General

1.1 The cloud service contract should include the agreed upon service levels. Additionally, all Service Level Agreements should be reviewed by a banking institution or microfinance 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 cloud service agreement with the third parties involved in cloud computing must define the third party's contractual obligation as guardian of a bank's data.

1.3 A banking institution or microfinance banking institution must ensure that the cloud service contract 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 or microfinance banking institution and the cloud service providers should understand how the data ownership rights are affected by the different laws of the countries which will host the data, with such understanding being documented.

2.3 For material cloud services and cloud services involving customer information, banking institutions or microfinance banking institutions must be aware of the location (city and country) where their data will be hosted and shall ensure that:

2.3.1 They consider the risk of foreign authorities having access to their data and require the cloud service provider to advise of instances where such service provider was legally bound to disclose clients' data to foreign authorities in the past and of any such potential disclosures in the future (if available) in their risk assessment.

2.3.2 The governing law and jurisdiction chosen are suitable for the enforceability of the contractual provisions in case of a breach thereof on the part of the cloud service provider.

2.3.3 The foreign jurisdiction's laws or regulations do not place any restrictions regarding:

(a) on-site examination audit and access rights of the Bank, the banking institution or microfinance banking institution, its external auditors or any third party appointed by them; and

(b) access to the information by the Bank, the banking institution, its external auditors or any third party appointed by them.

2.3.4 There are appropriate contractual provisions allowing the banking institution or microfinance banking institution to terminate the cloud service agreement where there is a change in location where their data is hosted, and they have concerns with the new location where the data is proposed to be hosted.

2.3.5 The authorities of countries where the data will be hosted, processed and managed or where the cloud service providers will be located, do not have automatic access to the data of the banking institution or microfinance banking institution. Where the cloud service provider is required to disclose data of the banking institution or microfinance banking institution to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction, the agreement entered with the cloud service providers must contain the following obligations to cater for such instances:

(a) the cloud service provider must use reasonable efforts to notify the banking institution or microfinance banking institution before any such disclosure is made, thereby enabling the banking institution to seek legal assistance as appropriate, to prevent or limit such disclosure, except to the extent where providing such prior notice to the banking institution or microfinance banking institution is prohibited by law or regulatory authority; and

(b) where the cloud service provider is unable to give such prior notice due to legal or regulatory constraints, it should implement appropriate legal and protective measures in the interest of the banking institution.

2.3.6 The Bank is duly and promptly informed by the banking institution or microfinance banking institution of any disclosure made by the cloud service provider in the event the latter is required to disclose data of the banking institution or microfinance banking to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction.

2.4 A banking institution or microfinance banking institution must 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 agreement in line with the banking institution's regulatory and legislative compliance requirements.

2.5 The contractual agreement must 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 must further clearly state that the service provider remains liable for performance in terms of the contract despite any subcontracting arrangements. Banking institutions or microfinance banking institutions must further ensure that:

2.5.1 They are aware of all subcontracting arrangements of the cloud service provider;

2.5.2 They duly understand the risks arising from the sub-contracting and comply with the relevant requirements of this Determination;

2.5.3 The sub-contractor is subject to relevant due diligence, controls and information security requirements that are commensurate with the nature of the services and the underlying risks considering the requirements of this Determination; and

2.5.4 They are provided with adequate notice in respect of changes in material subcontracting arrangements.

2.6. The service provider must provide an undertaking to treat the banking institution or microfinance 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 or microfinance 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 must 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 must 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 way.

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

3.5 All legal documents pertaining to the cloud service provision arrangements must be maintained in accordance with the banking institution or microfinance banking's institution legal document management procedures and legislative requirements.

4. Termination

4.1 A banking institution or microfinance 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 or microfinance banking institution should document the hardware, software and procedural requirements for moving from an existing service provider to another service provider or in-house.

5.2 A banking institution or microfinance banking institution must ensure that an exit from the cloud computing arrangement does not affect its compliance with any legislative or regulatory 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 of both parties at the termination of the agreement, including the circumstances when a banking institution enters into a resolution arrangement.

6.3 The contractual agreement should define how the agreement is to be terminated as well as the guarantees provided to enable the banking institution or microfinance 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 or microfinance banking institution's data be promptly and completely removed and returned to the banking institution or microfinance banking institution, transferred to another service provider as selected by a banking institution or microfinance banking institution or destroyed, depending on the nature of the data involved.

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 microfinance banking institution or create additional complexity in a resolution.

7.2 Where activities, functions or data outsourced are identified in a banking institution or microfinance banking institution's recovery plan, the banking institution or microfinance 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 cloud computing relationship as well as actions required to ensure continuity during recovery of the banking institution or microfinance banking institution or failure of the cloud 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 if a recovery or resolution action is taken.

8. Interoperability

8.1 A banking institution or microfinance banking institution must include interoperability as part of its cloud strategy and Service Level Agreements with Cloud Service Providers.

8.2 As part of its business continuity planning and testing, a banking institution must 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 A banking institution or microfinance banking institution must have contingency plans in place to continue with its operations in case of an unforeseen event, irrespective of whether a cloud environment has been deployed. The banking institution or microfinance banking institution's risk management processes must 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 prescribe the access that a banking institution, regulatory authorities and law enforcement agencies would have to conduct forensic audits and investigations.

9.2 The contractual agreement must prescribe how forensic evidence is made available to the banking institution or microfinance banking institution as well as the controls in place as proof that such evidence has not been compromised.

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

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

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

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

APPENDIX C

Banking institutions are required to complete the standardised template, BIR 301, upon reporting security incidents, breaches and significant outages to the Bank for systems and services hosted on the Cloud Service Provider.

Schedule I: Compliance with the Determination

	Proposed cloud service		**Response**
1.	Please provide a description of the proposed cloud services, including details on:		
	i. type of IT assets involved;		
	ii. chosen cloud service model;		
	iii. chosen cloud deployment model;		
	iv. activities/functions to be hosted on the cloud; and		
	v. the proposed date of commencement of the arrangement		
	Governance Framework		**Response**
2.	Cloud Strategy and Policy	Is there a board-approved cloud strategy and policy which is in line with the requirements under section 7 of the Determination?	
3.		Is the proposed use of cloud service in line with the board-approved cloud strategy and policy of the banking institution?	
4.	Board Approval	Has the approval of the board been obtained for the proposed use of cloud service?	
5.		Has the report specified under section 8.2(b) of the Determination been submitted to the board?	

6.	Responsibilities of Senior Management	Did the senior management comply with the requirements set out under section 7.3 of the Determination?	
7.	Oversight	Has an assessment of the adequacy of the internal resources for effective oversight of the cloud services been conducted?	
8.		Please provide the Shared Responsibility Matrix for the service.	
	Risk Management		**Response**
9.	Did the risk assessment cover the following:		
	i. identification of the associated risks (including cyber and IT related risk and concentration risk by the cloud service provider and by geographical location), the benefits and the sustainability of the cloud services and the impact on the risk profile of the banking institution;		
	ii. evaluation of criticality and sensitivity of the IT assets and the materiality of the services;		
	iii. evaluation of the impact of changes required to processes and procedures;		
	iv. evaluation of the adequacy of the internal cyber and/ or technology risk management framework including availability and adequacy of the skilled and experienced in-house resources for an effective deployment and oversight of the cloud services;		
	v. assessment to determine whether a privately managed environment on a virtual private network is required where the banking institution intends to opt for a public cloud for hosting customer information;		
	vi. identification of the roles and accountabilities of the banking institution and the cloud service provider under the shared responsibility model;		
	vii. assessment of the adequacy of the control framework;		
	viii. impact of possible risk events including failure of the cloud service provider, disruption of services, exit and the implications for transferring services in-house or to another cloud service provider, if required;		
	ix. adequacy of contingency and exit plan including the interoperability and portability of data and services;		
	x. risk of foreign authorities having access to a banking institution or microfinance banking institution's data; and		
	xi. relevant regulatory and legislative requirements?		
10.	Did the banking institution perform a vulnerability assessment and address all identified gaps?		
	Materiality Assessment		**Response**
11.	Has the board approved the criteria to assess the materiality of cloud services?		
12.	Were the following factors considered in the assessment of materiality:		
	i. the nature (including criticality) of the services and the IT assets;		
	ii. the potential direct and/or indirect impact that a confidentiality breach failure or disruption of the services could have on the institution and its customers. This includes the ability of the banking institution to meet its legal and regulatory requirements to continue its business operations and provide its services;		
	iii. the cost of the services as a share of total operating costs;		
	iv. the degree of difficulty in finding or migrating to an alternative provider or to bring the services in-house;		
	v. the potential impact of the service on current and projected earnings, solvency, liquidity, funding and capital and risk profile; and		
	vi. the ability to maintain appropriate internal controls and meet regulatory requirements in case of operational failures by the cloud service provider?		
	Due Diligence on Cloud Service Provider		**Response**
13.	Please provide the name of the cloud service provider.		
14.	Please specify the type of cloud service provider (third-party or intra-group entity)		
15.	Has the due diligence conducted been documented and approved?		
16.	Were the following factors considered in the due diligence exercise:		

	i. the adequacy of the cloud service provider's risk management and internal control systems, information security capabilities, and security controls including the controls for protecting the	
	confidentiality, integrity and availability of data;	
	ii. the cloud service provider's compliance with the requirements of this Determination, the applicable data protection, confidentiality and information security regulations or other legislations and adherence to international IT standards;	
	iii. the willingness and ability of the cloud service provider to service commitments even under adverse conditions, for instance, in the event of a cyber-attack or data theft;	
	iv. the ability of the cloud service providers to recover outsourced systems and IT services within the stipulated recovery time objective;	
	v. the verification of whether the personnel of the cloud service provider (including employees and subcontractors) with access to customer information are subject to adequate background screening, security training, access approvals and confidentiality arrangements as allowed by applicable law;	
	vi. forward-looking assessment of the financial and operational resilience of the cloud service provider; and	
	vii. an assessment of the proven track record of at least three years of the cloud service provider for such services?	
17.	Did the banking institution take into consideration the findings of any vulnerabilities assessment, penetration testing, audit and/or other reviews provided by the cloud service provider, where relevant?	
	Contractual Obligations	**Response**
18.	Is the agreement between the cloud service provider and the banking institution in line with all the requirements set out under section 12 of the Determination?	
19.	What is the applicable law governing the agreement?	
20.	Has the banking institution ensured that the agreement with the cloud service provider does not consist of clauses that would hinder the Bank from exercising its supervisory powers?	
21.	Does the agreement contain appropriate provisions to ensure Data Protection?	
22.	Does the agreement contain appropriate provisions for:	
	i. the right of audit (including remote audit) by the Bank, the banking institution, its external auditor, or any third party appointed by the Bank, the banking institution or its external auditor and the right of access to relevant audit reports and reports of other tests conducted by the cloud service provider;	
	ii. the obligation of the cloud service provider to cooperate with the Bank and provide access to information required by the Bank, the banking institution, its external auditor, or any third party appointed by the Bank; and	
	iii. the right of the Bank or any third party appointed by the Bank to promptly take possession of all the cloud services and data relating to the banking institution in the event the Bank decides	
	to revoke the licence of the banking institution or take any other action it considers fit to resolve the failing institution?	
	Cloud Security Management	**Response**
23.	Does the banking institution meet all the requirements set out under section 7 of the Determination?	
24.	Please provide the type of network connection used for data transmission between the institution and the cloud service provider and the network security measures employed therein, accompanied by a detailed network diagram.	
	Review, Audit, Testing and Control Functions	**Response**
25.	Are the reviews, audits, testing and control functions performed in line with the requirements under sections 9.1, 9.2 and 11 of the Determination?	
26.	What is the schedule of audit, testing and other reviews to be conducted by the banking institution and the cloud service provider?	
	Certifications and standards	**Response**
27.	Which Information security standards does the cloud service provider meet? (e.g. PCI DSS, ISOxx, etc…)	
28.	What certifications does the cloud service provider possess?	

	Data Location and Data Management		Response
29.	Does the banking institution meet all the requirements under Appendix B, 2. in respect of data location?		
30.	Has the assessment under Appendix B, 2.3 of the Determination been conducted by a competent officer of the banking institution or a reputed firm?		
31.	Has due diligence been conducted on the countries where the data will be hosted?		
32.	Does the cloud service provider make provision for law enforcement access based on a policy defined and agreed between the banking institution and the cloud service provider?		
33.	Please provide details on data protection laws that the cloud service provider adheres to.		
34.	Are Personally Identifiable Information (PII) protected?		
35.	Data at rest	Are the data at rest encrypted?	
36.		What is the encryption strength?	
37.	Data in transit	Is the data in transit encrypted?	
38.		What is the encryption strength?	
39.	Processing data	Are data processed in a secured environment?	
40.	Data Ownership/Access	What are the measures in place to ensure the retention of ownership rights of the data on the cloud?	
41.		What are the measures in place to prevent unauthorised access to confidential	
		Information?	
co42.	Data location	Specify the geographic locations where the data is:	
		i. processed.	
		ii. stored.	
43.	Terms and usage of cloud service	Describe the data and usage terms of the cloud service.	
44.	Exporting data	What are the methods available for exporting data?	
45.	Protocols for sharing/ interfacing	What are the permissible methods for sharing or interfacing with cloud data?	
46.	Data examination	Describe how the cloud service provider examines or monitors the data of the banking institution.	
	Contingency Plans, Exit Strategies, Service and Performance		**Response**
47.	Are the contingency plans for the proposed cloud service in line with the requirements under section 10 of the Determination?		
48.	Do the exit plans for the proposed cloud service cover all the requirements of section 12.6 of the Determination?		
49.	Termination of services	Is there a clear process for service termination? (e.g. Exit plan)	
50.		How long does it take for a full data wipeout? What are the arrangements in place for wiping of data?	
51.		How and when is the banking institution notified after data deletion?	
52.		What are the alternative solutions or arrangements that have been identified should the services be terminated?	
53.	Service	Are there clear mechanisms for monitoring the cloud services being provided?	
54.		What is the latency on the network?	
55.		What is the network bandwidth throughput?	
56.	Availability	What is the percentage of time that the service is available and usable?	
57.	Elasticity	How fast can the cloud service provider provision or adjust a given service?	
58.	Service resilience	What are the fault tolerance levels and methods put in place by the cloud service provider? (e.g. Network resilience, Data resilience, etc…)	

59.	Disaster recovery	What is the maximum time taken to perform a disaster switch in case of a system outage?	
60.		What is the Recovery point objective?	
61.		What is the Recovery time objective?	
62.		What are the fallback measures banking institutions or microfinance banking institutions intend to take in case network connectivity between Namibia and the outside world is disturbed for more than 1 hour?	
63.	Backup and restore	What are the provided methods of backup?	
64.		What is the backup retention period?	
65.		Does the backup utility adhere to the banking institution or microfinance banking's backup policy?	
66.		Are the backups encrypted?	
67.		What is the encryption strength?	
68.		What is the location of the backup storage?	
69.	Support	What type of support packages are available?	
70.		What is the chosen level of support?	
71.		What is the support service channel? (ticketing system, phone, email…)	
72.		What are the notification and alerting methods provided?	
73.		Is there a change request channel?	
74.	Incident management	Is there an incident management process in place?	
75.		Are incident reports provided?	
	Subcontracting (as applicable)		
76.	Please provide the name of the sub-contractor for material cloud services.		
77.	Has due diligence been conducted on the sub-contractor?		
78.	Have the requirements under Appendix B, 2.5 of the Determination been met?		
	Concentration Risk Management		**Response**
79.	Please provide an assessment of the suitability of the cloud service provider's substitutability and the portability of the data or services on the cloud as easy, moderate or extremely difficult		
80.	What are the measures taken to mitigate concentration risk:		
	i. by the cloud service provider; and		
	ii. by geographical location?		

Schedule II: Shared Responsibility Matrix

	Cloud Services		
Components	**Infrastructure as a Service**	**Platform as a Service**	**Software as a Service**
Content	Banking Institution Managed	Banking Institution Managed	Banking Institution Managed
On-going monitoring of control effectiveness	Banking Institution Managed	Banking Institution Managed	Banking Institution Managed
Data quality	Banking Institution Managed	Banking Institution Managed	Banking Institution Managed
Identity and Access Management	Banking Institution Managed	Banking Institution Managed	Banking Institution Managed
Application Security	Banking Institution Managed	Banking Institution Managed	Cloud Service Provider Managed
Deployment	Banking Institution Managed	Banking Institution Managed	Cloud Service Provider Managed

Privileged User Management	Banking Institution Managed	Banking Institution Managed	Cloud Service Provider Managed
Runtime	Banking Institution Managed	Cloud Service Provider Managed	Cloud Service Provider Managed
Patching	Banking Institution Managed	To be defined/Agreed mutually	Cloud Service Provider Managed
Penetration Testing	Banking Institution Managed	To be defined/Agreed mutually	Cloud Service Provider Managed
Disaster Recovery Testing	Banking Institution Managed	To be defined/Agreed mutually	Cloud Service Provider Managed
Network Security & Controls	Banking Institution Managed	To be defined/Agreed mutually	Cloud Service Provider Managed
SIEM and Audit Logging	Banking Institution Managed	To be defined/Agreed mutually	Cloud Service Provider Managed
Virtualisation	To be defined/Agreed mutually	Cloud Service Provider Managed	Cloud Service Provider Managed
OS Management	To be defined/Agreed mutually	Cloud Service Provider Managed	Cloud Service Provider Managed
Storage	Cloud Service Provider Managed	Cloud Service Provider Managed	Cloud Service Provider Managed
Hardware	Cloud Service Provider Managed	Cloud Service Provider Managed	Cloud Service Provider Managed