BANK OF MAURITIUS

Guideline on Use of Cloud Services

7 September 2022

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

INTRODUCTION

The use of cloud services can offer a number of advantages such as economies of scale, flexibility as well as greater operational and cost efficiencies. However, it may expose financial institutions to additional risks.

This Guideline sets out:

i. the general requirements for the use of cloud services; and

ii. the additional minimum requirements for the use of material cloud services and for cloud services which involve customer information.

Financial institutions are expected to follow a risk-based approach in respect of cloud services. The level of governance to be applied, the risk assessment, the information security requirements, the types of controls to be deployed, the contingency plans and exit strategies as well as the level of the initial and on-going due diligence and assurance to be performed shall be commensurate with the materiality of the services.

Financial institutions shall have a phased and prudent deployment for material cloud services. They should comply with all the requirements of this Guideline and implement additional controls in light of latest international standards and best practices for material cloud services.

Financial institutions should also comply with the Guidelines on Outsourcing by Financial Institutions in the event the use of cloud services includes an outsourced activity.

Purpose

The purpose of this Guideline is to provide the necessary guidance to financial institutions engaging in the use of cloud services such that the risks are duly identified and managed.

Authority

This Guideline is issued under the authority of section 50 of the Bank of Mauritius Act 2004, section 100 of the Banking Act 2004 and section 17 of the National Payment Systems Act 2018.

Scope of application

This Guideline applies to all cloud-based arrangements entered by any financial institution licensed by the Bank under the Banking Act 2004 and the National Payment Systems Act 2018.

Effective date

This Guideline shall come into effect on 7 September 2022.

Interpretation[1]

"Bank" means the Bank of Mauritius established under the Bank of Mauritius Act 2004;

"board" means the board of directors of a financial institution except for branches of foreign banks where "board" means the local advisory board/committee. For branches of foreign banks with no local advisory board, the responsibilities assigned to the board shall rest on the Chief Executive Officer of the branch;

"control functions" mean those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function;

"cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction;

"cloud infrastructure" refers to the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer;

"cloud services" refer to services provided using cloud computing. For the purpose of this Guideline, cloud services may be provided through the following different types of *cloud deployment model*:

i. *hybrid cloud*: a cloud service/infrastructure that is composed of two or more distinct deployment models or services that retain unique infrastructures but are interconnected;

ii. *private cloud*: a cloud infrastructure where computing resources are used solely by one single organisation, either physically in the company's on-site data centre(s) (on-premises) or externally with the third-party provider (hosted private cloud). In the latter case, a virtual private network is typically set up between the company and the third-party cloud provider. In both scenarios, services are not accessible or even publicly visible over the internet; and

iii. *public cloud*: a cloud infrastructure that is available for open use by the general public;

"cloud service model" refers to the type of computing resource that is offered. There are three main types of cloud service model:

i. *Infrastructure as a Service (IaaS)*: Providers offer access to computer infrastructure resources such as processing power, storage, servers, networks and other resources where users are able to run an operating system with applications of their choice on it.

[1] Largely based on definitions by the National Institute of Standards and Technology (NIST), the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS) and the Financial Stability Board (FSB)

Virtualisation allows many users to share one physical server. Users have control over storage levels, operating system and specific network components;

ii. *Platform as a Service (PaaS)*: Providers offer a computing platform where users can run and develop their own applications using libraries, languages, databases, tools and other providers' resources. This option provides users with tools for developing new online applications. Users have control only of their own applications that run on the platform plus the platform's configuration settings; and

iii. *Software as a Service (SaaS)*: Providers offer access to application software from any device with an internet connection and web browser. Off-the-shelf applications are free or paid via a subscription, accessed over the internet from any device, facilitating collaborative working. Users have control only of configuration settings specific to the application;

"cloud service provider" refers to the entity hosting the cloud services or infrastructure;

"containers" refer to lightweight packages of application code together with dependencies such as specific versions of programming language runtimes and libraries required to run a software service;

"financial institution" for the purpose of this Guideline refers to:

i. any bank, non-bank deposit taking institution, cash dealer or payment service provider licensed by the Bank; or

ii. any operator of a payment system, clearing system or settlement system, authorised by the Bank;

"hypervisor" means hardware and software used to create and run Virtual Machines allowing multiple operating systems to run concurrently on a single host computer;

"Information Technology (IT) asset" refers to any piece of data, device or other component of the environment that supports IT-related activities. For the purpose of this Guideline, IT assets shall include data, hardware, software, computer processing, network and storage;

"outsourcing" has the same meaning as in the Guidelines on Outsourcing by Financial Institutions;

"material cloud service" for the purpose of this Guideline, refers to:

i. a service of such importance that any weakness or failure in the provision of this activity could have a significant impact on the financial institution's ability to meet its regulatory responsibilities and/or to continue in business and/or cause a significant disruption in business operations of the financial institution; or

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

iii. a service involving critical or sensitive IT assets; or

iv. any other service which meets the materiality criteria as approved by the board of the financial institution; and

"virtualisation" means the act of creating a virtual (rather than actual) version of something, including but not limited to a virtual computer hardware platform, operating system, storage device or computer network resources.

1. Governance Framework

1.1 Cloud Strategy

1.1.1. Financial institutions that use or intend to use cloud services shall have a board-approved cloud strategy setting out:

i. the IT assets under consideration (categorised by sensitivity and criticality) and the intended cloud deployment model and cloud service model to be applied;

ii. the underlying rationale including expected benefits and costs and the associated risks;

iii. the adequacy of the existing cyber and technology risk management framework and the appropriateness of the skills and knowledge of internal staff (including on-going training requirements) for an effective deployment and oversight of the cloud services; and

iv. the requirements to ensure that there is no undue concentration on single cloud service providers or geographical locations for material cloud services.

1.2 Policy for Use of Cloud Services

1.2.1. Financial institutions that use or intend to use cloud services shall establish a comprehensive risk-based board-approved policy on such services, either on a stand-alone basis or integrated within relevant existing policies.

1.2.2. The policy shall be risk-based and shall, as a minimum, take into consideration the requirements stipulated in this Guideline.

1.2.3. The policy shall be aligned with the overall information technology (IT) / cloud strategy and risk appetite of the financial institution.

1.2.4. The policy shall be reviewed at least on an annual basis or at such higher frequency as may be required in anticipation of or subsequent to material events.

1.3 Board Oversight

1.3.1 The board shall retain the ultimate responsibility to ensure that:

i. the cloud services are conducted in a safe and sound manner and in compliance with relevant laws and regulations; and

ii. the associated risks are duly identified, understood, monitored and mitigated.

1.3.2 The board shall be responsible for:

i. approving the cloud strategy and policy on the use of cloud services;

ii. approving the criteria to assess the materiality of the cloud services;

iii. approving and overseeing material cloud services and ensuring that there is an appropriate business continuity and contingency/exit plan for such services;

iv. setting out the appropriate approval authorities for the use of non-material cloud services;

v. ensuring that it is duly apprised of all cloud services at the outset and on an on-going basis, and that it is promptly informed of any critical issue and incident;

vi. ensuring that the policy is aligned with the overall information technology (IT) strategy, cloud strategy, architecture and risk appetite of the financial institution and takes into consideration the relevant regulatory and legislative requirements;

vii. 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;

viii. ensuring that there is an appropriate risk assessment framework and adequate oversight and coverage by the control functions and the external auditors;

ix. ensuring that the board, senior management and other relevant staff have the adequate level of expertise and experience and are provided with the relevant training for an effective oversight of the cloud services;

x. ensuring that the board and the audit committee receive periodic report on audit, testing and reviews required under section 8 of the Guideline and that it is satisfied with the risk mitigating actions/remediation plans; and

xi. ensuring that it receives a comprehensive report on any proposed material cloud service covering, inter alia:

    a. compliance with the requirements of the Guideline as well as the board-approved cloud strategy and policy on use of cloud services of the financial institution;

    b. the governance and assurance frameworks including arrangements for audit, testing and other reviews;

    c. the risk assessment;

    d. the due diligence on the cloud service provider and on the data location;

    e. details of the responsibilities and accountabilities of the financial institution and the cloud service provider;

    f. adequacy of security arrangements/controls both on-premise and on cloud;

    g. arrangements for business continuity, exit and in the event the Bank decides to revoke the licence of the financial institution or appoints a conservator;

h. availability of internal resources/training plans for an effective deployment and oversight;

i. measures in place for the financial institution to meet its regulatory obligations and other legal and regulatory requirements and to access the IT assets on cloud; and

j. rights of the Bank in respect of its supervisory powers.

1.4 Branches and Subsidiaries of Foreign Banks

1.4.1 Branches and subsidiaries of foreign banks may adopt the cloud strategy and policy on the use of cloud services of their parent bank provided that they are in line with the requirements of this Guideline. Branches of foreign banks which do not have a local advisory board or committee shall 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 bank.

1.5 Responsibilities of Senior Management

1.5.1 The senior management of the financial institution shall, as a minimum, oversee the design, development and implementation of cloud services and ensure that:

i. the policy for use of cloud services is duly documented and approved by the board;

ii. a thorough risk assessment is conducted prior to the use of cloud services;

iii. the design of the cloud-based arrangement, the security architecture deployed in the cloud environment, the risk mitigating measures and other controls in place are robust and adequate to address the identified risks at the outset and on an on-going basis. As a minimum, the security controls on cloud shall be as stringent as the controls in the on-premise environment;

iv. there is an independent evaluation of the security arrangements in place, on-premise and in the cloud environment as well as of the business continuity plans prior to the implementation of the cloud-based arrangement and on an on-going basis;

v. where the financial institution intends to opt for a public cloud for hosting customer information, the risk management framework takes into consideration the characteristics which are unique to public cloud and the selected cloud service model;

vi. there is a clear delineation of the responsibility and accountability between the financial institution and the cloud service provider, that the responsibilities resting on the financial institution are well understood and managed and that the responsibilities of the service provider are duly managed with appropriate oversight from the financial institution. A Cloud Shared Responsibility Matrix is provided under Schedule II of the Annex for guidance;

vii. the board is kept informed of the implementation status and on-going performance of cloud services as well as of any current or emerging risks and issues; and

viii. there is an ongoing monitoring of the performance of the cloud services and timely identification, escalation and reporting of incidents.

2. Risk Assessment

2.1 The risk assessment shall be duly documented and shall include, among others:

i. identification of the associated risks (including cyber/IT related risk and concentration risk by cloud service provider and by geographical location), the vulnerabilities, the benefits and the sustainability of the cloud services and the impact on the risk profile of the financial 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/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 financial institution intends to opt for a public cloud for hosting customer information;

vi. identification of the roles and accountabilities of the financial institution and the cloud service provider under the shared responsibility model;

vii. assessment of the adequacy of the control framework;

viii. the impact of possible risk events including failure of cloud service provider, disruption of services, exit and the implications for transferring services in-house or to another cloud service provider, if required;

ix. the adequacy of contingency and exit plan including the interoperability and portability of data and services;

x. the risk of foreign authorities having access to its data; and

xi. the relevant legal and regulatory requirements.

3. Materiality Assessment

3.1 Financial institutions shall, as a minimum, consider the following factors in their assessment of materiality:

i. the nature (including the criticality) of the services and of the IT assets;

ii. the potential direct/ indirect impact that a confidentiality breach or failure or disruption of the services could have on the institution and its customers. This includes the ability of the financial institution to meet its legal and regulatory requirements and 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 to find or migrate 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 service provider.

4. Regulatory Notification

4.1 Financial institutions shall notify the Bank of the proposed deployment of material cloud services.

4.2 The notification shall be done at least 60 days before the proposed deployment of the cloud services and shall be accompanied by an attestation from the Chief Executive Officer of the financial institution confirming, inter alia, the approval of the board and compliance with the Guideline together with the information listed in Schedule I of the Annex.

4.3 Where the use of cloud services also involves outsourcing of activities, financial institutions shall include any additional information required under the Guidelines on Outsourcing by Financial Institutions in their notification.

4.4 In case material cloud services are subcontracted, financial institutions shall also provide relevant details on the subcontractor in their notification. The Bank shall be duly notified of any subsequent material changes in material subcontracting arrangements. In both cases, the notification shall be accompanied by a confirmation that the financial institution has complied with all requirements under section 11 of the Guideline.

5. Due Diligence on Cloud Service Provider

5.1 Financial institutions shall conduct due diligence on cloud service providers before using their service.

5.2 The extent of due diligence to be performed, including the requirements for onsite audits or remote audits, shall be commensurate with materiality of the services and of the IT assets involved and the level of reliance that the financial institution places on the cloud service provider to maintain effective security controls.

5.3 The due diligence on a cloud service provider in respect of material cloud services shall, inter alia, include:

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 taking into consideration the findings of vulnerabilities assessment, penetration testing, audit and/or other reviews provided by the cloud service provider, where relevant;

ii. the cloud service provider's compliance with the requirements of this Guideline, 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 and recovery point 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.

5.4 The due diligence shall be duly documented and approved.

6. Contractual Obligations

6.1 Financial institutions shall not engage into a cloud service without entering into a written agreement with the cloud service provider and shall ensure that all agreements contain appropriate clauses on access to information stored on cloud by the financial institution and the Bank. For subsidiaries and branches of foreign banks, the agreement may comprise master agreements entered by the respective foreign banks together with relevant addendum for the local entity.

6.2 Financial institutions shall ensure that all agreements for material cloud services and cloud services involving customer information:

i. do not consist of clauses that would hinder the Bank from exercising its supervisory powers;

ii. contain appropriate provisions to ensure compliance with the Mauritian data protection laws (Data Protection Act 2017, ICTA, etc) or to data protection laws which are equivalent to the Mauritian data protection laws at all times; and

iii. impose confidentiality obligations on the cloud service provider which are in line with the underlying objective of section 64 of the Banking Act 2004 or section 18 of the National Payment Systems Act 2018.

6.3 Agreements for material cloud services shall also, inter alia, include relevant clauses on

i. the right of audit (including remote audit) by the Bank, the financial institution, its external auditors, or any third party appointed by the Bank, the financial 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 audit by any third party appointed by the Bank shall be borne by the financial institution;

ii. the obligation of the cloud service provider to cooperate with the Bank and provide access to information required by the Bank, the financial institution, its external auditors, or any third party appointed by the Bank;

iii. the arrangements to ensure smooth exit and transition to a new service provider or bringing the service in-house;

iv. the arrangements to ensure compliance with the record keeping obligations as set out in the Banking Act 2004;

v. the obligation of the cloud service provider to provide reasonable notice in the event of changes in subcontractor or change in location where the data is stored or processed;

vi. 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 financial institution in the event the Bank decides to revoke the licence of the financial institution or appoints a conservator. The procedures for executing the change of ownership request and for ensuring continuity of services during this process should be duly documented and agreed with the cloud service provider;

vii. the right of the financial institution to terminate the agreement where, inter alia, the financial institution has concerns on the cloud service provider, the location of the data and the subcontractors involved;

viii. the obligation of the cloud service provider in respect of prompt deletion of information at the end of the life cycle of the IT assets or upon exit;

ix. incident management process, including the roles and responsibilities of each party;

x. the governing law; and

xi. dispute resolution considering the chosen governing law for the contract.

7. Cloud Security Management

7.1 Financial institutions shall 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 information and other IT assets involved, the nature of the service, the classification of data, the location of data, the cloud deployment model and the cloud service model.

7.2 For material cloud services, financial institutions shall, as a minimum:

i. be aware of the information security measures and controls established by the cloud service provider and/or any international IT standards that the service provider adheres to;

ii. establish procedures for regular assessment of vulnerabilities to their IT system and prescribe minimal standards for such assessments, for instance, identification of weak security configurations, open network ports and application vulnerabilities;

iii. ensure that the security controls for the cloud infrastructure are equivalent, if not more stringent than the controls in the on-premise environment of the financial institution. Financial institutions may choose to leverage on available cloud security services to assist with managing and monitoring security for cloud services;

iv. ensure that the cloud service provider is able to provide assurance that it has appropriate controls over the hypervisor, or any other virtual infrastructure controls used by the service provider to manage the cloud services being provided to the financial institution. This may include, inter alia, verifying whether the cloud service provider scans its hypervisor code for vulnerabilities and monitors system logs;

v. implement appropriate safeguards against risks arising from virtualisation. Financial institutions shall ensure that all components of a virtualisation solution have the same level of security and resilience as a non-virtualised IT environment. This includes implementing strong access controls to restrict administrative access to the hypervisor and host operating system, as well as establishing policies and standards to manage virtual machines images and snapshots;

vi. establish an inventory management process to track and manage IT assets residing on the cloud;

vii. have in place identity and access management, access logs and network controls that are commensurate with the materiality of the IT assets and risks involved. This may include, inter alia, limiting account privileges, implementing multifactor authentication/dual control, frequently updating and reviewing account access list, and implementing tools designed to detect unauthorised access for material IT assets;

viii. ensure that data stored on the cloud and in transit and the channel to access them are encrypted and that the level of encryption are commensurate with the materiality of IT assets, the cloud deployment model and risks involved. The encryption keys shall be stored separately from virtual images and the data;

ix. have in place an encryption key management process. The financial institution may hold the encryption key and manage encryption through the use of hardware security modules, virtual encryption tools, cloud-based security tools or a combination of these or retain the cloud-based key management services of a reputed third-party service provider provided that it ensures that there are appropriate arrangements in place to secure the keys. Where the financial institution opts for the cloud-based key management services of the cloud service provider hosting its data, it shall ensure that:

    a. there is appropriate segregation within the cloud service provider between access to keys and access to customer information; and

    b. it understands and is satisfied with the circumstances in which the cloud service provider may use or access the encryption keys;

x. control access to encryption keys for core banking services. The financial institution may grant the cloud service provider access to the encryption keys to deliver pre-agreed critical/security services;

xi. ensure that their data is segregated, sufficiently protected and can be clearly identified;

xii. ensure that container-specific security controls are implemented where containers are used in the cloud computing environment. This may include, inter alia:

    a. storing data outside of the container, so that the data does not have to be re-created when updating and replacing containers;

    b. verifying that configurations prevent containers from unintentionally interacting;

    c. securing containers from applications within them;

    d. securing the host from containers and vice versa; and

    e. monitoring containers for vulnerabilities and updating or replacing containers when appropriate;

xiii. ensure that they are aware of security, reliability, and latency issues related to the use of microservices where they use microservice architecture for cloud application development. In this respect, financial institutions shall evaluate implementation options prior to using microservices and ensure that such options are within their risk appetite and that they have appropriate security controls in place;

xiv. ensure secure Application Programming Interfaces (APIs) are deployed;

xv. ensure that an appropriate incident management process is in place that sets out the roles and responsibilities of each party in this respect; and

xvi. ensure a centralised visibility and control of their core components on the cloud which include but are not limited to:

    a. identity and access management;

    b. databases;

    c. security;

    d. encryption and keys; and

    e. backups;

xvii. ensure that all network connectivity is point to point and encrypted;

xviii. ensure that interfacing data centres from Mauritius have dual connectivity to the cloud service provider from two or more distinct Internet Service Providers using different network path;

xix. ensure that there are appropriate logs/ audit trails;

xx. mitigate concentration risk through:

    a. the implementation of a multi-cloud strategy for different material cloud services and the development of appropriate contingency plans, including portability and interoperability solutions (in house or to another cloud service provider) to mitigate concentration risk by cloud service provider;

    b. the selection of geographically separated data centres to address concentration risk by geographical location; and

    c. the utilisation of frequent server instance back-ups or data redundancy replication, and storage of data within multiple geographic regions as well as across multiple Availability Zones within each region; and

xxi. with respect to the use of public cloud, implement:

    a. robust logical isolation controls to ensure that their data is virtually segregated from other cloud tenants;

b. the highest level of security features offered by the cloud service provider taking into consideration best international practices and standards;

c. data object encryption, file encryption or tokenisation in addition to encryption provided at platform level for data at rest;

d. session encryption or data object encryption in addition to encryption provided at platform level for data in motion;

e. confidential computing solutions which isolate sensitive data in a protected, hardware-based computing enclave during processing for data in use; and

f. robust Identity and Access Management (IAM) controls (dual factor authentication including One-Time Password) wherein access to public cloud services and IT assets is assessed and granted on a per-request and need-to basis.

8. Review, Audit, Testing and Control Functions

8.1 The scope and frequency of the review, testing and audits shall be risk-based taking into consideration the materiality of the cloud services and the IT assets. For material cloud services, the frequency shall not exceed 18 months and financial institutions shall implement a higher frequency if required in anticipation of or subsequent to material events.

8.2 Financial institutions shall ensure that the information security controls on premise and on cloud are subject to regular and appropriate testing and audits. This may include, but not limited to, penetration tests, vulnerability assessments, internal audit or third-party audits.

8.3 Financial institutions shall conduct a review of all material cloud services and cloud services involving customer information. The scope of the review shall, at least, include:

i. a comprehensive end-to-end assessment of risks and corresponding controls including oversight in relation of cloud services;

ii. verification that cloud service providers continue to meet their contractual, legal and regulatory obligations; and

iii. verification that the cloud services comply with the requirements of this Guideline and the board-approved policy on use of cloud services of the financial institution.

8.4 Financial institutions may, as part of their review, audits or testing, take into consideration third-party assessments, third-party certifications and third-party audit reports by independent parties or rely on pooled audits organised jointly with other clients of the same cloud service provider, and performed by these clients or by an independent third party appointed by them.

8.5 Where there is reliance on third-party audit reports or testing/assessment performed by the cloud service provider or any other third party which has not been appointed by the financial institution, it shall, among others:

i. be satisfied with the plan and the scope of the audit/assessment and the reports;

ii. be satisfied with the independence, skills and aptitude of the third party conducting the audit/testing/assessment;

iii. ensure that IT systems and key controls are duly covered; and

iv. assess the contents of the report and take actions as appropriate.

8.6 Financial institutions shall have robust control functions with adequate resources and expertise and ensure that the control functions adequately cover the processes with respect to the use of cloud services.

8.7 Financial institutions shall ensure that its compliance function, its internal audit function and its external auditors conduct a periodic review of material cloud services and cloud services involving customer information.

8.8 Financial institutions shall perform a vulnerability assessment and ensure that all identified gaps are duly addressed prior to the deployment or redeployment of material cloud services.

8.9 Financial institutions shall conduct a penetration testing immediately after the deployment of material cloud services.

9. Data Location

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

i. they consider the risk of foreign authorities having access to their data and require the cloud service provider to advise of instances where it 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;

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

iii. data protection laws in the foreign jurisdiction where the data is hosted and processed are in line with the Mauritian data protection laws or data protection laws which are equivalent to the Mauritian data protection laws;

iv. 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 financial institution, its external auditors or any third party appointed by them; and

    b. access to the information by the Bank, the financial institution, its external auditors or any third party appointed by them;

v. there are appropriate contractual provisions allowing the financial institution to terminate the agreement in case there is a change in location where their data is hosted and they have concerns with the new location;

vi. 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 access to the data of the financial institution. Where the cloud service provider is required to disclose data of the financial 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 should contain the following obligations to cater for such instances:

    a. the cloud service provider shall use reasonable efforts to notify the financial institution before any such disclosure is made so that the financial institution may seek by legal means to prevent or limit such disclosure, except to the extent that providing such prior notice to the financial 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 financial institution; and

vii. the Bank is duly informed by the financial institution of any disclosure made by the cloud service provider in the event the latter is required to disclose data of the financial 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.

9.2 Financial institutions shall ensure that the assessment under section 9.1 is conducted by a competent officer of the financial institution or a reputed firm, as deemed appropriate.

9.3 Financial institutions shall establish a pre-agreed list of locations where its data will be processed with the cloud service provider. Where data is processed in a location outside the pre-agreed list, the financial institution shall ensure that:

i. such instances are limited to cases involving processing of individual transactions initiated by end users of the financial institution;

ii. it is promptly informed by the cloud service provider of the location (city and country) where its data has been processed including the rationale thereof; and

iii. it obtains assurance from the cloud service provider that the processing of data was done in a secured environment and that its data has been permanently removed from that location and transferred to a pre-agreed location within a reasonable timeframe.

10. Contingency Plans and Exit Strategies

10.1 For material cloud services, financial institutions shall ensure that:

i. business continuity requirements such as disaster recovery plans, recovery time, recovery point objectives, maximum allowable loss of data, plans for communicating incidents and the frequency of testing of adequacy and effectiveness of these plans are developed, documented and, where appropriate, agreed with the cloud service provider;

ii. the business continuity plans of the cloud service provider are regularly tested. The business continuity plan of the cloud service provider shall be ideally certified or mapped to internationally recognised standards;

iii. appropriate system resiliency and network redundancy in the event of disaster are catered for in the cloud-based arrangements. Such network redundancy and resilience capabilities shall be tested regularly;

iv. the cloud service provider has adequate plans and resources to ensure the financial institution's continuity of operations, including recovery and resumption capabilities; and

v. comprehensive and well documented exit strategies are established and regularly reviewed to ensure that they remain adequate and effective. The exit plan shall, as a minimum, include the following:

a. agreed process and procedures including reasonable timeframe for deletion of all data (bank and customer data) of the financial institution;

b. assurance from the cloud service provider through relevant independent reports/certificates that all data of the financial institution (including any backup) is rendered permanently irrecoverable and inaccessible in a timely manner after termination of the contract;

c. transferability of services (to a third party or back to the financial institution) for the purpose of continuity of service; and

d. identification of alternative solutions to allow for business continuity throughout and after the transition phase.

11. Subcontracting

11.1 With respect material cloud services, financial institutions shall ensure that:

i. they are aware of all subcontracting arrangements of the cloud service provider;

ii. they duly understand the risks arising from the sub-contracting and comply with the relevant requirements of this Guideline;

iii. 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 Guideline; and

iv. they are provided with adequate notice in respect of changes in material subcontracting arrangements.

12. Record-Keeping and Reporting Requirement

12.1 Financial institutions shall keep an updated register of information on all their cloud services, irrespective of their materiality.

12.2 Financial institutions shall submit to the Bank a Return on Use of Cloud Services, in such form and manner prescribed by the Bank.

12.3 Financial institutions shall report promptly to the Bank any incident including unauthorised access or breach of confidentiality and security, directly or indirectly, by a cloud service provider.

13. Transitional arrangement

13.1 Financial institutions shall comply with the requirements of this Guideline for new cloud-based services.

13.2 Financial institutions shall ensure:

i. the establishment of the requisite strategy, policy and processes within 6 months of the effective date of this Guideline; and

ii. compliance with the remaining requirements of this Guideline for existing cloud services within 12 months from the effective date of this Guideline.

Bank of Mauritius
7 September 2022

ANNEX

Schedule I

Compliance with the Guideline

	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 cloud; and		
	v. the proposed date of commencement of the arrangement		
	Governance Framework		**Response**
2.	Cloud Strategy & Policy	Is there a board-approved cloud strategy which is line with the requirements under section 1.1.1 of the Guideline?	
3.		Is the proposed use of cloud service in line with the board-approved cloud strategy and policy of the financial institution?	
4.	Board Approval	Has the approval of the board been obtained for the proposed use of cloud service?	
5.		Has the report under section 1.3.2 (xi) of the Guideline been submitted to the board?	
6.	Responsibilities of Senior Management	Did the senior management comply with the requirements set out under section 1.5.1 of the Guideline?	
7.	Oversight	Has an assessment of the adequacy of the internal resources for an effective oversight on 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/IT related risk and concentration risk by 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 financial 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/technology risk management framework including availability and adequacy of the skilled and experienced in-house resources for an effective deployment and oversight on the cloud services;		

	v. assessment to determine whether a privately managed environment on a virtual private network is required where the financial institution intends to opt for a public cloud for hosting customer information;	
	vi. identification of the roles and accountabilities of the financial institution and the cloud service provider under the shared responsibility model;	
	vii. assessment of the adequacy of the control framework;	
	viii. the impact of possible risk events including failure of cloud service provider, disruption of services, exit and the implications for transferring services in-house or to another cloud service provider, if required;	
	ix. the adequacy of contingency and exit plan including the interoperability and portability of data and services;	
	x. the risk of foreign authorities having access to its data; and	
	xi. the relevant regulatory and legislative requirements?	
10.	Did the financial institution perform a vulnerability assessment and address all identified gap?	
	Materiality Assessment	**Response**
11.	Has the board approved the criteria to assess materiality of cloud services?	
12.	Were the following factors considered in the assessment of materiality:	
	i. the nature (including criticality) of the services and of the IT assets;	
	ii. the potential direct/ indirect impact that a confidentiality breach or failure or disruption of the services could have on the institution and its customers. This includes the ability of the financial institution to meet its legal and regulatory requirements and 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 to find or migrate 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 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 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, 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 guideline, 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 financial institution take into consideration the findings of 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 financial institution in line with all the requirements set out under section 6 of the Guideline?	
19.	What is the applicable law governing the agreement?	
20.	Has the financial 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 compliance with the Data Protection Act 2017?	
22.	Does the agreement contain confidentiality obligations which are in line with the underlying objective of section 64 of the Banking Act 2004?	
23.	Does the agreement contain appropriate provisions on:	
	i. the right of audit (including remote audit) by the Bank, the financial institution, its external auditor, or any third party appointed by the Bank, the financial institution or its external auditor and right of access to relevant audit reports/ 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 financial 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 financial institution in the event the Bank decides	

	to revoke the licence of the financial institution or appoints a conservator?		
	Cloud Security Management		**Response**
24.	Does the financial institution meet all the requirements set out under section 7 of the Guideline?		
25.	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**
26.	Are the reviews, audits, testing and control functions performed in line with the requirements under section 8 of the Guideline?		
27.	What is the schedule of audit, testing and other reviews to be conducted by the financial institution and the cloud service provider?		
	Certifications and standards		**Response**
28.	Which Information security standards does the cloud service provider meet? (e.g. PCI DSS, ISOxx, etc…)		
29.	What certifications does the cloud service provider possess?		
	Data Location and Data Management		**Response**
30.	Does the financial institution meet all the requirements under section 9 in respect of data location?		
31.	Has the assessment under section 9.1 of the Guideline been conducted by a competent officer of the financial institution or a reputed firm?		
32.	Has a due diligence been conducted on the countries where the data will be hosted?		
33.	Does the cloud service provider make provision for law enforcements access based on a policy defined and agreed between the financial institution and the cloud service provider?		
34.	Does the cloud service provider adhere to Mauritian data protection laws (e.g. DPA 2017, ICTA, etc…) or to data protection laws which are equivalent to the Mauritian data protection laws? If no, please provide details on data protection laws that the cloud service provider adheres to.		
35.	Are Personally identifiable Information (PII) protected?		
36.	Will personal data be exported? If yes, have the requirements under the DPA 2017 been met?		
37.	Data at rest	Are the data at rest encrypted?	
38.		What is the encryption strength?	
39.	Data in transit	Are the data in transit encrypted?	
40.		What is the encryption strength?	
41.	Processing data	Are data processed in a secured environment?	
42.	Data Ownership/Access	What are the measures in place to ensure retention of ownership rights of the data on cloud?	
43.		What are the measures in place to prevent unauthorised access to confidential	

		information?	
44.	Data location	Specify the geographic locations where the data is:	
		i. processed.	
		ii. stored.	
45.	Terms and usage of cloud service	Describe the data and usage terms of the cloud service.	
46.	Exporting data	What are the methods available for exporting data?	
47.	Protocols for sharing/interfacing	What are the permissible methods for sharing/interfacing with cloud data?	
48.	Data examination	Describe how does the cloud service provider examine/monitor data of financial institution?	
	Contingency Plans, Exit Strategies, Service and Performance		**Response**
49.	Are the contingency plans for the proposed cloud service in line with the requirements under section 10 of the Guideline?		
50.	Do the exit plans for the proposed cloud service cover all the requirements of section 10 of the Guideline?		
51.	Termination of services	Is there a clear process for service termination? (e.g. Exit plan)	
52.		How long does it take for a full data wipe out? What are the arrangements in place for wiping of data?	
53.		How and when is the financial institution notified after deletion?	
54.		What are the alternative solutions/arrangements that have been idenfied?	
55.	Service	Are there clear mechanisms for monitoring the cloud services being provided?	
56.		What is the latency on the network?	
57.		What is the network bandwidth throughput?	
58.	Availability	What is the percentage time that the service is available and usable?	
60.	Elasticity	How fast can the cloud service provider provision or adjust a given service?	
61.	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…)	
62.	Disaster recovery	What is the maximum time taken to perform a disaster switch in case of a system outage?	
63.		What is the Recovery point objective (RPO)?	
64.		What is the Recovery time objective (RTO)?	
65.		What are the fallback measures FIs intend to take in case network connectivity between Mauritius and the outside world is disturbed for more than 1 hour?	

66.	Backup & restore	What are the provided methods of backup?	
67.		What is the backup retention period?	
68.		Does the backup utility adhere to your backup policy?	
69.		Are the backups encrypted?	
70.		What is the encryption strength?	
71.		What is the location of the backup storage?	
72.	Support	What type of support packages are available?	
73.		What is the chosen level of support?	
74.		What is the support service channel? (ticketing system, phone, email…)	
75.		What are the notification and alerting methods provided?	
76.		Is there a change request channel?	
77.	Incident management	Is there an incident management process in place?	
78.		Are incident reports provided?	
	Subcontracting (as applicable)		
79.	Please provide the name of the sub-contractor for material cloud services.		
80.	Has a due diligence been conducted on the sub-contractor?		
81.	Have the requirements under section 11 of the Guideline been met?		
	Concentration Risk Management		**Response**
82.	Please provide an assessment of the suitability of the cloud service provider's substitutability and of the portability of the data/ services on cloud as easy, moderate or extremely difficult.		
83.	What are the measures taken to mitigate concentration risk:		
	i. by cloud service provider; and		
	ii. by geographical location?		

Schedule II

	Cloud Services		
Components	**IaaS**	**PaaS**	**SaaS**
Content	FI Managed	FI Managed	FI Managed
On-going monitoring of control effectiveness	FI Managed	FI Managed	FI Managed
Data quality	FI Managed	FI Managed	FI Managed
Identity & Access Management	FI Managed	FI Managed	FI Managed
Application Security	FI Managed	FI Managed	CSP Managed
Deployment	FI Managed	FI Managed	CSP Managed
Privileged User Management	FI Managed	FI Managed	CSP Managed
Runtime	FI Managed	CSP Managed	CSP Managed
Patching	FI Managed	To be defined/Agreed mutually	CSP Managed
Penetration Testing	FI Managed	To be defined/Agreed mutually	CSP Managed
Disaster Recovery Testing	FI Managed	To be defined/Agreed mutually	CSP Managed
Network Security & Controls	FI Managed	To be defined/Agreed mutually	CSP Managed
SIEM & Audit Logging	FI Managed	To be defined/Agreed mutually	CSP Managed
Virtualisation	To be defined/Agreed mutually	CSP Managed	CSP Managed
OS Management	To be defined/Agreed mutually	CSP Managed	CSP Managed
Storage	CSP Managed	CSP Managed	CSP Managed
Hardware	CSP Managed	CSP Managed	CSP Managed