`

**BANK OF MAURITIUS**

# Guideline on Use of Cloud Services



**Month 2021**

*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 challenges stemming from data protection and location, security issues and concentration risk.

This Guideline sets out the general principles for the use of cloud services. It also lays down the minimum requirements that shall be applicable to the use of cloud services provided by third parties for material services. Where specified in the Guideline, these minimum requirements shall also apply to 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 information security requirements, the types of controls to be deployed, as well as the level of the initial and on-going, due diligence and assurance to be performed shall be commensurate with the criticality of the services.

Financial institutions should also comply to the Guideline on Outsourcing by Financial Institutions in the event an outsourced activity avails of the use of cloud services.

### 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 appropriately identified and managed.

### Authority

This Guideline is issued under the authority of section 50 of the Bank of Mauritius Act 2004 and section 100 of the Banking Act 2004.

### 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.

### Effective date

This Guideline shall come into effect on xx Month 2021.

### Interpretation

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

"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. For the purposes of this Guideline, cloud deployment models shall include public cloud, private cloud, hybrid cloud and dedicated cloud;

"cloud services" refer to services provided using cloud computing;

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

main types of service model:

i. *Infrastructure as a Service (IaaS)*: Providers offer access to computer infrastructure resources 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. 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.

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;

"dedicated cloud" means a cloud infrastructure, which essentially is an isolated and dedicated zone of the public cloud where services and/or infrastructure are provided through a single tenant architecture for the organisation;

"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;

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

"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" means recourse to a third-party service provider, which may be an entity that is related or unrelated to the financial institution, to perform on a continuing basis a business

activity, service, function or process, which would normally be undertaken by the financial institution itself, now or in the future;

"material 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 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;

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

iv. any other service classified as material under the Guideline on Outsourcing by Financial Institutions;

"private cloud" means 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;

"public cloud" means a cloud infrastructure that is available for open use by the general public; 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:

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

b. the underlying rationale including expected benefits and cost and the associated risks;

c. 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 on the cloud services;

d. the requirements to ensure that there is a phased and prudent deployment of material activities; and

e. the requirements to ensure that there is no undue concentration on single cloud service providers or geographical locations for material 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 of directors of the financial institution shall retain the ultimate responsibility to ensure that:

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

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

1.3.2 The board of directors shall, as a minimum, be responsible for:

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

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

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

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

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

f. 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;

g. ensuring that the deployment of cloud services is in line with the model set out in Schedule IV;

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

i. ensuring that the board of directors, senior management and other relevant staff have the adequate levels of expertise and experience and are provided with appropriate and on-going training for an effective oversight of the cloud services; and

j. ensuring that the board of directors and the audit committee receives 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.

### 1.4 Responsibilities of Senior Management

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

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

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

c. 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;

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

e. 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 III of the Annex for guidance;

f. the board of directors 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

g. there is an ongoing monitoring of the performance 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:

a. identification of the associated risk (including concentration risk), the benefits and the sustainability of the cloud services and the impact on the risk profile of the financial institution;

b. evaluation of criticality and sensitivity of the IT assets and the materiality of the services;

c. evaluation of the impact of changes required to processes and procedures;

d. 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;

e. assessment to determine whether a dedicated cloud is required where the financial institution intends to opt for a public cloud for hosting customer information;

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

g. assessment of the adequacy of the control framework;

h. 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;

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

j. the relevant regulatory and legislative requirements.

## 3. Materiality Assessment

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

a. the criticality of the services and of the IT assets;

b. 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;

c. the cost of the services as a share of total operating costs;

d. the degree of difficulty to find or migrate to an alternative provider or to bring the services in-house;

e. the potential impact of service disruption on the ability of the financial institution to continue to provide its services; and

f. any other criteria specified in the Guideline on Outsourcing by Financial Institutions in this regard.

## 4. Material Services

4.1 Financial institutions shall seek the prior authorisation of the Bank for material cloud services. Such request for approval shall be accompanied by the information requirements listed in Schedule I of the Annex.

4.2 For material cloud services, financial institutions shall ensure:

a. compliance with all the requirements set out in this Guideline;

b. implementation of additional controls which are commensurate with the criticality of the service;

c. a phased and prudent deployment of such services;

d. compliance with the deployment model set out in Schedule IV; and

e. a proven track record of at least three years of the cloud service provider.

## 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 criticality/sensitivity of the services and of the IT assets involved and the level of reliance 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 services shall, inter alia, include:

a. 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;

b. 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;

c. 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;

d. the ability of the cloud service providers to recover outsourced systems and IT services within the stipulated recovery time objective;

e. 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;

f. forward looking assessment of the financial and operational resilience of the cloud service provider; and

g. the track record 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 clause on access to information stored on cloud by the financial institution and the Bank.

6.2 Financial institutions shall ensure that all agreements for material cloud services and

non-material cloud services involving customer information:

a. contain appropriate provisions regarding compliance with relevant confidentiality/data protection laws and regulations, including the requirement of section 64 of the Banking Act; and

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

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

a. the right of access of the Bank for conducting on-site or remote examinations at the cloud service providers or data centres, subject to reasonable notice being provided to the cloud service provider unless this is not possible due to an emergency or crisis situation. The cost of on-site or remote examinations shall be borne by the financial institution;

b. the right of audit (including remote audit) by 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 service provider. The cost of audit by any third party appointed by the Bank shall be borne by the financial institution;

c. the obligation of the cloud service provider to cooperate with the Bank;

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

e. 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;

f. the right of the Bank or any third party appointed by the Bank to promptly take possession of all the services and the IT assets 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 should be duly documented and agreed with the cloud service provider;

g. the right of the financial institution to terminate the agreement;

h. the obligation in respect of prompt deletion of information at the end of the life cycle of the IT assets or upon exit; and

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

## 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 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 and services involving customer information, 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 systems 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 criticality 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 critical IT assets;

viii. ensure that data stored on the cloud and in transit and the channel to access them are encrypted, that the level of encryption be commensurate with the materiality of data and risks involved and that the cloud service provider does not have access to the encryption keys for information relating to customers. The encryption keys shall be stored separately from virtual images and IT assets. Financial institutions shall have in place an encryption key management process and may opt to:

    a. retain 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

    b. retain the cloud-based key management services of a reputed third-party service provider, other than the cloud service provider and any party related or connected to the cloud service provider;

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

x. 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;

xi. 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;

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

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

xiv. ensure a centralised visibility and control of their core components on the cloud

which include but are not limited to the following:

a. identity and access management;

b. databases;

c. security;

d. encryption and keys; and

e. backups.

## 8. Review, Audit, Testing and Control Functions

8.1 Material cloud services and cloud services involving customer information shall be reviewed on an annual basis or at such higher frequency as may be required in anticipation of or subsequent to material events. 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.

8.2 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. The scope and frequency of the testing and audits shall be risk-based, taking into consideration the materiality of the cloud-based services and the criticality of the assets, but shall not exceed 12 months.

8.3 Financial institutions may, as part of their review, audits or testing, take into consideration third-party assessment, 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.

8.4 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.

8.5 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.

8.6 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.

## 9. Data Location

9.1 Financial institutions shall be aware of the exact location where their data will be hosted and shall ensure that:

i. contractual provisions are recognised in the foreign jurisdiction and can be enforced in the chosen jurisdiction;

ii. data standards in the foreign jurisdiction are in accordance with the laws and regulations in the jurisdiction of the financial institution;

iii. foreign jurisdiction’s laws or regulations restrict access to information on the cloud and to the cloud service provider's business premises to any unauthorised third party;

iv. dispute resolution with the cloud service provider is possible in the jurisdiction of the cloud service provider;

v. foreign jurisdiction’s laws or regulations do not place any restrictions:

a. on-site examination audit and access right of the Bank, the financial institution, its external auditor or any third party appointed by them; and

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

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.

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.

## 10. Contingency Plans and Exit Strategies

10.1 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; and

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

10.2 Financial institutions shall establish exit strategies that are comprehensive, well-documented. Exit plans 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.

10.3 Financial institutions shall ensure that the exit plans are regularly reviewed to ensure that they remain adequate and effective.

## 11. Subcontracting

11.1 All requirements applicable to the cloud services under this Guideline shall apply to the services which are sub-contracted.

11.2 Financial institutions shall ensure that they are able to maintain similar control over the

risks arising from their cloud-based arrangements in the event a cloud service provider relies on a sub-contractor to support services.

11.3 The sub-contractor shall be subject to equivalent due diligence, controls and information security requirements as the cloud service provider.

11.4 Financial institutions shall ensure that they are provided with adequate notice in respect of changes in subcontracting arrangements for material services. In the event the subcontracting arrangement required the approval of the Bank, the financial institution shall ensure that the prior authorisation of the Bank is sought before the changes in the subcontracting arrangement take effect.

## 12. Reporting Requirement

12.1 Financial institutions shall submit to the Bank a Return on Use of Cloud-based Services/Activities, containing a list of all material and non-material cloud-based services/activities in such form and manner prescribed by the Bank on an annual basis. The annual return should be submitted within the next twenty working days of the previous calendar year. In the event of any change, the amended return shall be submitted within a week following the change.

12.2 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 and the action/s it is proposed to take in consequence.

## 13. Transitional arrangement

13.1 A transitional period of six months shall be granted to all financial institutions to ensure compliance with the requirements of the Guideline.

**Bank of Mauritius**
**Xx xxxx 2021**

**ANNEX**

## Schedule I
## Information to be provided when seeking the approval of the Bank

(i) A description of the proposed cloud services, including details on the type of IT assets involved, the type of cloud service model and cloud deployment model to be used;

(ii) A risk assessment report of the services on cloud, including the proposed risk mitigating controls;

(iii) The name of the cloud service provider and the organisational structure of its group, where applicable;

(iv) The name of the sub-contractor, where applicable;

(v) Due diligence report on the cloud service provider/ country where the third party is registered and where the data is processed and hosted;

(vi) The type of cloud service provider (third party or intra-group entity);

(vii) A description of the activities and IT assets to be hosted on cloud;

(viii) The proposed date of commencement of the cloud-based arrangement;

(ix) 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;

(x) The applicable law governing the outsourcing agreement;

(xi) The business continuity plan for the services;

(xii) The exit strategy;

(xiii) An assessment of the adequacy of the internal resources for an effective oversight on the cloud services;

(xiv) The date and results of the last penetration test, vulnerability assessment, internal audit reports and other relevant reports;

(xv) The date when the continuity plan was last tested and the results thereof;

(xvi) The completed questionnaire as per Schedule II;

(xvii) The Shared Responsibility Matrix for the service and an assessment of the adequacy and appropriateness of the security arrangement at the cloud service provider and the financial institution; and

(xviii) 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.

## Schedule II

| Governance | | Response |
|---|---|---|
| Approval | Has the approval of the board of directors been obtained? | |
| Policies and regulations | Does the Cloud Service Provider (CSP) adhere to Mauritian data protection laws? (e.g. DPA 2017, ICTA, etc…) | |
| | Are Personally identifiable Information (PII) protected? | |
| | Which Information security standards does the CSP meet? (e.g. PCI DSS, ISOxx, etc…) | |
| Termination of services | Is there a clear process for service termination? (e.g. Exit plan) | |
| | How long does it take for a full data wipe out? | |
| | How and when is the Financial Institution (FI) notified after deletion? | |
| Change / deprecate Features | What is the average time taken for the implementation of a feature required by a governing body? | |
| | What is the average time taken for a retirement of a feature required by a governing body? | |
| Access to law enforcement and authorities | Does the CSP make provision for law enforcements access based on a policy defined and agreed between the FI and the CSP? | |
| Audits | Are audit policies defined? | |
| | What certifications does the CSP possess? | |
| | What is the schedule of audits? | |
| **Service and Performance** | | **Response** |
| Service | Are there clear mechanisms for monitoring the cloud services being provided? | |
| | What is the latency on the network? | |
| | What are the average and maximum response time? | |
| | What is the number of simultaneous user connection possible? | |
| | What is the network bandwidth throughput? | |

| | | |
|---|---|---|
| Availability | What is the percentage time that the service is available and usable? | |
| | What is the Mean time between failures? | |
| Elasticity | How fast can the CSP provision or adjust a given service? | |
| Service resilience | What are the fault tolerance levels and methods put in place by the CSP? (e.g. Network resilience, Data resilience, etc…) | |
| Disaster recovery | What is the maximum time taken to perform a disaster switch in case of a system outage? | |
| | What is the Recovery point objective (RPO)? | |
| | What is the Recovery time objective (RTO)? | |
| | Have recovery procedures been developed? | |
| | How often are those recovery procedures tested? | |
| | 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? | |
| Backup & restore | What are the provided methods of backup? | |
| | What is the backup retention period? | |
| | Does the backup utility adhere to your backup policy? | |
| | Are the backups encrypted? | |
| | What is the encryption strength? | |
| | Are restoration procedures available? | |
| | How often are restoration tests done? | |
| | What is the location of the backup storage? | |
| Support | What type of support packages are available? | |
| | What is the chosen level of support? | |
| | What is the support service channel? (ticketing system, phone, email…) | |
| | What are the notification and alerting methods provided? | |
| | Is there a change request channel? | |
| | Are incident reports provided? | |
| **Data management** | | **Response** |

| | | |
|---|---|---|
| Data Ownership/Access | What are the measures in place to ensure retention of ownership rights of the data on cloud? | |
| | What are the measures in place to prevent unauthorised access to confidential information? | |
| Data location | Specify the geographic locations where the data is: | |
| | Processed | |
| | Stored | |
| Data stored | List all data fields stored on the cloud (names, addresses, etc.). | |
| Mapping to Mauritian data regulations | Provide a table of mappings for prevailing country's data regulation onto Mauritian data protection laws. | |
| | | |
| | | |
| Terms and usage of cloud service | Describe the data and usage terms of the cloud service. | |
| Exporting data | What are the methods available for exporting data? | |
| Protocols for sharing/interfacing | What are the permissible methods for sharing/interfacing with cloud data? | |
| Data examination | Describe how does the CSP examine/monitor FI data? | |
| **Agreement between FI and CSP** | | |
| Does the agreement contain appropriate provisions on: | | |
| Right of access | the right of access of the Bank to the information relating to the financial institution and for conducting on-site or remote examinations by the Bank at the cloud service providers or data centres, at any time? | |
| Onsite examination/audit | the right for onsite examination by the Bank, the right of audit (including remote audit) by 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 service provider? | |
| Cooperation | the obligation of the cloud service provider to cooperate with the Bank? | |
| Exit/transition | the arrangements to ensure smooth exit and transition to a new service provider or bringing the service in-house? | |
| Change in subcontractor or location | 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 | |
| Change of ownership | the right of the Bank or any third party appointed by the Bank to promptly take possession of all the services and the IT assets in the event the Bank decides to revoke the licence of the financial institution or appoints a conservator? | |
| Deletion of data | the obligation in respect of prompt deletion of information at the end of the life cycle of the IT assets or upon exit? | |
| Incident management | incident management process? | |

## Schedule III

| | 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 |

**Schedule IV**

| Materiality | Cloud Service Model | Cloud Deployment Model | | | |
|---|---|---|---|---|---|
| | | Public Cloud | Private Cloud | Hybrid Cloud | Dedicated Cloud |
| Non-Material Service | IaaS | | | | |
| | PaaS | | | | |
| | SaaS | | | | |
| Material Service | IaaS | | | | Network connectivity between FI and data centre point-to-point and encrypted. |
| | PaaS | | | | Network connectivity between FI and data centre point-to-point and encrypted. |
| | SaaS | | | Data should reside on either a private cloud or a single-tenant. Network connectivity between FI and data centre point-to-point and encrypted. | Network connectivity between FI and data centre point-to-point and encrypted. |

| Key | |
|---|---|
| | Allowed with conditions |
| | Allowed |
| | Not allowed |
| | Not applicable |

Conditions:

1. Irrespective of materiality, network traffic encryption between the CSP and the FI is mandatory in all cloud deployment models.
2. Data encryption for material services and services containing customer information is mandatory for both data at rest and in transit.
3. Core banking services shall be considered as being material given its criticality and shall be hosted on a private cloud. However, the Bank may approve, on a case-to-case basis, requests to host core banking services on a dedicated cloud provided that the

financial institution is able to demonstrate to the Bank that it has adequate controls in place.