Financial Services Commission
MAURITIUS

FINANCIAL SERVICES COMMISSION

GUIDELINES

CLOUD COMPUTING SERVICES

29 June 2023

1.0 INTRODUCTION

1.1 The Financial Services Commission, Mauritius ('FSC') has, during the course of its offsite and onsite monitoring, noted that licensees are increasingly using cloud computing services (as defined in the **Appendix** to this document) to access various types of software/hardware tools and applications.

1.2 These Guidelines, issued pursuant to the powers conferred to the FSC under section 7(1)(a) of the Financial Services Act 2007 ('FSA'), aim to provide general guidance to licensees regarding their use of cloud computing services.

1.3 Consequently, in addition to ensuring compliance with the provisions of the Data Protection Act 2017, the Computer Misuse and Cybercrime Act 2003 and the Information and Communication Technologies Act 2001, licensees will be required to apply the best practices laid out in these Guidelines, while taking into consideration the nature, scale and complexity of their business activities, environment and risks respectively.

1.4 The FSC may direct any licensee or any other person, to comply with these Guidelines and failure to do so may entail regulatory actions and constitute an offence.

2.0 CLOUD STRATEGY AND POLICY FORMULATION

2.1 Licensees making use of cloud computing services are required to implement a risk-based cloud strategy and policy which addresses the following aspects:

i. the Information Technology (IT) assets under consideration, the cloud-based service being acquired as well as the cloud deployment model being used. For instance, licensees shall determine whether a privately managed cloud infrastructure on a private network is suitable for hosting customer information;

ii. the underlying rationale, including anticipated benefits and costs, as well as the associated risks;

iii. the cloud risk management framework, including cyber security and data protection in accordance with the legal and regulatory requirements in place; and

iv. the appropriate skills and expertise of internal staff (including on-going training) for a successful running of the cloud-based service deployment and on-going monitoring.

2.2 The cloud strategy and policy should be approved by the Board of directors and reviewed, on a regular basis (i.e. at least once every year or, as may be required in anticipation of or subsequent to any material event).

3.0 CLOUD RISK MANAGEMENT FRAMEWORK

3.1 Licensees shall establish and maintain, at all times, a robust risk management framework to *inter-alia* identify, assess, manage, mitigate and report the risks associated with the adoption of cloud computing services.

3.2 Such risk management framework shall be well-documented and take into consideration:

i. the vulnerabilities and benefits, including the adequacy and sustainability of the cloud computing services and the implementation impact and/or any changes required thereto;

ii. the cybersecurity, IT and concentration risks which are relevant to the cloud service provider and its geographical locations (for example, through data encryption, access control, network security, and incident response processes);

iii. the evaluation of criticality and sensitivity of the IT assets;

iv. the evaluation and appropriateness of the skills and expertise of internal staff;

v. the identification of the roles and responsibilities of the licensee and the cloud service provider under the outsourcing arrangement;

vi. the impact of possible risk events, including the disruption of services, failure of the cloud service provider, exit and implications of transferring services in-house or to an alternate service provider;

vii. the adequacy of the business contingency plan and exit strategy, including the interoperability and portability of data and services; and

viii. the relevant legal and regulatory frameworks.

3.3 The risk management framework shall be aligned with the materiality assessment framework (refer to Section 4.0 below).

4.0 CLOUD MATERIALITY ASSESSMENT

4.1 Licensees shall assess the materiality of the cloud computing services, taking into consideration the following factors:

i. the costs of the cloud computing services and IT assets, as part of total operational costs;

ii. the potential impact of the services on current and projected earnings, solvency, liquidity, funding and capital;

iii. the cost of transferring services in-house or migrating to an alternate service provider, if required;

iv. the potential impact of any unforeseen event, including any confidentiality breach or a disruption of the services, even a failure of the cloud service provider, which could have a direct or indirect impact on the licensee and its clients; and

v. the ability to maintain adequate internal controls and meet regulatory requirements and business continuity, including in case of any operational failure by the cloud service provider.

4.2 Licensees shall notify the FSC in writing, at least 15 business days prior to the deployment of any material cloud computing services.

5.0 CONTRACTUAL OBLIGATIONS

5.1 Licensees shall enter into a written contractual arrangement with cloud service providers regarding the cloud computing services being acquired. The written contractual arrangement shall contain relevant clauses pertaining to the cloud computing services, including:

i. a clear definition of the roles and responsibilities of the licensee and the cloud service provider, including the incident management process and dispute resolution process;

ii. the obligation of the cloud service provider to provide adequate information and access to data storage to the licensee, including in the event of changes in the location where the data is being stored or processed, or any change in the contractual arrangements;

iii. the obligation of the cloud service provider to provide a reasonable notice in the event of changes in location where the data is being stored or processed or any change in the contractual arrangements;

iv. the right of the licensee to terminate the contractual arrangements where, *inter-alia*, the licensee has concerns about the cloud service provider and the post exit strategy is agreed upon; and in this respect, the obligation to ensure that there is a smooth exit and transition to a new cloud service provider or the licensee itself; and

v. the arrangements to ensure compliance with the relevant laws and regulations of Mauritius.

5.2 The cloud service providers may subcontract their services to another service provider. The licensees shall, in that respect, ensure that:

i. the cloud service provider informs them within an adequate notice period on any new material subcontracting agreements or any changes in the existing arrangements; and

ii. the subcontractor is subject to appropriate due diligence, controls, and information security requirements that are relevant to the nature and underlying risks to the use of its services.

5.3 Notwithstanding any provisions of the sub-contracting agreement, the cloud service providers shall retain full legal liability for the cloud computing services acquired by the licensee.

6.0 DUE DILIGENCE ON CLOUD SERVICE PROVIDERS

6.1 As a matter of principle, whenever outsourcing any function, licensees are required to conduct appropriate due diligence to ensure that the delegate is fit and proper and has the capacity to fulfil the delegated/outsourced function.

6.2 Similarly, licensees shall conduct due diligence on cloud service providers prior to entering into any outsourcing arrangement and accepting their services respectively.

6.3 The due diligence shall be well-documented and *inter-alia* include:

i. the identification and verification of the cloud service provider through background screening;

ii. the appropriateness of the cloud service provider's risk management and internal control systems, information security and data protection capabilities, as well as security controls in place, while taking into account the findings of vulnerability assessments, penetration testing, audits, and/or other controls put in place by the cloud service provider, as appropriate;

iii. the extent to which the cloud service provider complies with the applicable laws and standards[1] governing data protection, confidentiality and information security;

iv. the readiness and ability of the cloud service provider to uphold its obligations under adverse conditions, such as in the event of a cyberattack or data theft; and

v. the ability of the cloud service provider to recover outsourced systems and IT services within the recovery time objective.

6.4 The extent of the due diligence to be performed, including the audit requirements, should be commensurate with the materiality of the cloud computing services and the level of reliance that the licensee places on the cloud service provider.

7.0 CLOUD SECURITY AND DATA MANAGEMENT FRAMEWORK

7.1 Licensees shall establish and maintain a cloud security management framework which would allow them to mitigate any cyber-risk and data vulnerability that may occur due to the use of the cloud computing services.

7.2 The cloud security management framework shall take into account the following elements:

i. information provided by the cloud service provider on its procedures, controls and audit reviews relating to the management and monitoring of the security system of the cloud computing services and infrastructure, including how the shared data are used, stored, transferred and/or processed in the cloud computing system;

ii. information provided by the cloud service provider on the countries whereby data are stored and information about the safeguards in place;

[1] E.g. ISO/IEC 27001 and related standards https://www.iso.org/isoiec-27001-information-security.html

iii. assurance from the cloud service provider that data-in-transit within the cloud infrastructure is secure. This will include data transferred between data centres located in different geographical regions;

iv. a security assessment of the cloud service provider conducted by a third-party as well as regular assessments of vulnerabilities to the cloud service provider's IT systems. The cloud service provider should normally indicate to the licensee the time line for its response when a security vulnerability is identified;

v. information about the cloud service provider's resilience capabilities including how quickly data can be restored (without alteration) from a backup, in the event of an incident or major data loss; and

vi. the encryption key management process put in place by the cloud service provider to ensure that data is segregated, sufficiently protected and can be clearly identified. The encryption keys and channelling of data should be stored separately, whilst taking into account the materiality of IT assets, the cloud deployment model and risks involved.

7.3 The security controls should be aligned with the nature and materiality of the cloud computing services, the criticality and sensitivity of information, as well as the classification and location of the data.

8.0 CONTINGENCY PLANS AND EXIT STRATEGIES

8.1 Licensees shall ensure that the cloud service provider has a comprehensive and well-documented contingency plan, such that there will be quick recovery and continuity of operations as a result of unforeseen events.

8.2 Such contingency plan and exit strategy shall include the following elements:

i. business continuity requirements, such as disaster or incident recovery plans to mitigate the loss of data, whilst ensuring that the cloud service provider has adequate resources to resume activities, after such events;

ii. adequate system resiliency and network redundancy for the purpose of continuity of operations.

8.3 Licensees shall have a well-designed exit strategy which shall, at a minimum, include the following:

i. agreed process and procedures on termination of agreement with the cloud service provider, including reasonable timeframe for the cloud service provider to delete all data of the licensee;

ii. procedures for the cloud service provider to transfer services to another service provider or back to the licensee; and

iii. identification of alternative solutions to be adopted for business continuity.

8.4 The contingency plans and exit strategies shall be reviewed at least once a year, to ensure that they remain adequate and effective.

9.0 AUDIT REVIEWS

9.1 Licensees shall follow a risk-based approach to the implementation of on-going controls and monitoring of the cloud service providers, whilst taking into account the materiality of the cloud computing services and the IT assets.

9.2 The scope and frequency of these on-going controls and monitoring shall be organised on a consistent basis.

9.3 Licensees shall, at least once a year, conduct a review of all material cloud computing services and ensure that:

i. the cloud service providers are subject to regular audits and testing of their procedures and comply with the Board approved policy on cloud computing services, the contractual agreements as well as the legal and regulatory obligations; and

ii. the staff performing the audit – internal auditors of the licensees or external auditors acting on their behalf – have the appropriate skills and knowledge to

properly assess the relevant cloud computing services and perform effective and relevant audits.

10.0 BOARD AND SENIOR MANAGEMENT RESPONSIBILITIES

10.1 The board of directors of the licensees shall ensure that it is not discharged of its responsibilities upon any delegation or outsourcing arrangement to a cloud service provider. It is accordingly responsible for:

i. approving the cloud strategy and policy on cloud computing services' arrangements;

ii. ensuring that the policy is aligned with the cloud strategy, the cloud deployment model and the risk appetite of the licensee;

iii. ensuring that the cloud risk management framework and adequate controls / security arrangements both in-premise and on cloud are in place;

iv. approving the criteria to assess the materiality of the cloud computing services, the material cloud computing services and the contingency strategy and exit plans, as appropriate;

v. ensuring that the business contingency plans and exit strategies are efficiently deployed in the event of any critical issue, unforeseen event and incident encountered with the adoption of the cloud computing services;

vi. ensuring that the implementation of cloud computing services complies with the record keeping obligations of the licensees, in accordance with section 29 of the FSA, including the maintenance of an updated physical or electronic register of information in relation to such services;

vii. ensuring that the licensee has the available resources and capabilities to use the cloud computing services, whilst providing adequate training to the relevant staff for an effective oversight of the cloud computing services; and

viii. ensuring that the board of directors and its audit committee receive a comprehensive periodic report relevant to the use of the cloud computing services.

10.2 The senior management of the licensees shall, in practice, subsequently provide effective oversight on the deployment of the cloud computing services and ensure that:

i. the cloud service providers are selected based on the licensee's needs and that proper due diligence, risk and materiality assessments are carried out prior to the adoption of cloud computing services;

ii. the cloud policy and strategy approved by the Board are duly documented;

iii. the design of the cloud computing arrangements, the security architecture deployed in the cloud computing environment, the cloud risk management framework, and other internal controls and procedures are in accordance with principles of sound corporate governance and risk management;

iv. there is a clear delineation of responsibility and accountability between the licensee and the cloud service provider, and that responsibilities of the cloud service provider are duly managed with appropriate oversight from the licensee;

v. an independent evaluation of the cloud security management and data protection arrangements put in place, on premise and in the cloud environment, are carried out on a regular basis; and

vi. there is an on-going monitoring of performance of the cloud computing services and timely identification, escalation and prompt reporting of incidents (including unauthorised access or breach of confidentiality and security, directly or indirectly, by a cloud service provider) to the Board, as well as to the FSC (by completing the template specified in the **Schedule**), in the eventuality of material incidents.

SCHEDULE

Cloud Computing Services (Material Incident Reporting)	
1. Licensee Details	
Date and time of notification to the FSC	
Full name of licensee	
Name of officer reporting the material incident	
• Designation and department	
• Contact details (email, mobile, office phone)	
Name of officer responsible for restoration of the systems and functions	
• Designation and department	
• Contact details (email, mobile, office phone)	
2. Details of Material Incident:	
Date and time of material incident occurrence and detection	
Who discovered the material incident? (e.g. *third-party service provider, customer, employee*)	
Nature of material incident and affected areas:	
(a) Outage of IT system (e.g. *back-end systems*)	
(b) Signs of cyber-attack (e.g. *Hacking or malware infection against the licensee's system, web defacement, distributed denial of service attacks*)?	
(c) Theft or Loss of Information (e.g. *sensitive/important/customer information stolen or missing from business locations*)	
(d) Unavailability of Infrastructure or work premises (e.g. *Power blackout, telecommunication*	

linkages down)	
(e) Others	
Where are affected systems located (on premises, on cloud etc.)?	
What actions have been taken by the licensee?	
What responses are planned?	
3. Impact (examples are given but not exhaustive):	
(a) Impact on business (*e.g. product offerings, services etc.*)	
(b) Impact on stakeholders (*e.g. affected customers, service providers etc.*)	
(c) Financial and market impact (*e.g. monetary losses etc.*)	
(d) Reputational impact – is the material incident likely to attract media attention?	
(e) Regulatory and Legal impact	
(f) Other impacts	

APPENDIX

In these Guidelines -

"*Cloud computing*" is a broad term which encompasses access to a shared pool of on-demand configurable computing resources over the internet. These resources are provided in various forms where minimal management effort or service provider interaction are required. The cloud computing services are offered in three main "cloud service models", namely:

a. **Software as a Service (SaaS)** - an application software hosted by a third-party provider and delivered to customers over the internet as a service. The application software typically takes the form of a standardised off-the-shelf application, which is free or paid via a subscription, and accessed over the internet from any device. Users have only permission to the configuration settings specific to the application;

b. **Platform as a Service (PaaS)** - the usage of computing platform where users may develop and run their own online applications using the tools, database and other providers' resources available. Users have only control over their own applications which runs on the platform; and

c. **Infrastructure as a Service (IaaS)** - the usage of computer infrastructure resources – whether physical or virtual servers, networking, storage, and data center space. Users have only control over the operating system, storage levels and specific networking components.

"*Cloud computing services*" or "*cloud-based services*" refer to the services provided from the usage of cloud computing against a "pay-per use" basis. These cloud services are provided through the following different deployment models:

a. **Public cloud**: the cloud infrastructure is owned and operated by the service provider and is accessible on a public network;

b. **Private cloud**: the cloud infrastructure is operated solely by a single organisation, either physically managed on-site data centre(s) (on-premises) or externally by a third party and hosted on a private network; and

c. **Hybrid cloud**: the cloud infrastructure is built on a private cloud architecture with strategic combination of public cloud services. It therefore retains some unique characteristics of the two infrastructures which are interconnected.

"*Cloud infrastructure*" refers to the essential characteristics of cloud computing, which may comprise of a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the provision of the cloud service, and typically includes servers, storage and network components. On the other hand, the abstraction layer consists of the software deployed across the physical layer.

"*Cloud service provider*" refers to the entity providing or hosting the cloud service models.

"*Licensee*" has the same meaning as in the FSA.

"*Material cloud service*" refers to any cloud computing services adopted by a licensee whose interruption is likely to have a significant impact on:

a. the licensee's ability to continue in business and/or cause a significant disruption in the business operations of the licensee;

b. the licensee's ability to meet its regulatory responsibilities and/or the conditions of its licence;

c. the licensee's ability to manage risks including risks relating to any unauthorised access or disclosure, loss or theft of customer information; or

d. any critical or sensitive assets of the licensee including IT assets.

"*Outsourcing*" means an arrangement whereby licensees engage a third-party service provider to perform activities on an ongoing basis that would normally have been undertaken by the licensees themselves.