OPERATIONAL RISK MANAGEMENT MODULE

MODULE	OM Operational Risk Management
	Table of Contents

Table of Contents (continued)

MODULE	OM:	Operational Risk Management
CHAPTER	OM-2A:	Cloud Outsourcing Arrangements

OM-2A.1 General Requirements

OM-2A.1.1 This Chapter sets out the CBB's requirements for material cloud outsourcing arrangements. CBB considers cloud services offered by Cloud Service Providers ("CSP") as a form of outsourcing and it recognises that licensees may leverage such services to reap the benefits of a CSP's infrastructure. Cloud services and solutions generally provide scalability, increased flexibility, help allocate resources more effectively, reduce operational and cost burden. However, the risks, particularly data protection and information security risks, need to be managed efficiently and effectively.

OM-2A.1.2 A cloud outsourcing arrangement refers to any arrangement between the conventional bank licensee and a CSP by which that CSP performs a function (operation, processes, services or activities) on behalf of the licensee.

OM-2A.1.3 **Conventional bank licensees must consider cloud outsourcing arrangements which, in the event of a service failure or security breach, have the potential to either materially impact a licensee's business operations, reputation, profitability or ability to manage risk and comply with applicable laws and regulations, or which involve 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 licensee's customers as material cloud outsourcing arrangements.**

OM-2A.1.4 **In order to assess if a cloud outsourcing arrangement is material, the following must be considered:**

(a) Whether the data hosted on cloud systems has the following characteristics:
1. **Personally identifiable customer or staff information such as payroll, bank account or credit card data;**
2. **Internal critical systems such as core banking, trading systems and risk management systems;**
3. **Non-public commercially sensitive information that could influence financial markets; and**
4. **Regulatory reporting or accounting data.**

(b) The criticality of the activities to be outsourced, i.e. are these activities critical to the business continuity/viability of the licensee and its obligations to customers;

(c) The impact of outages, and related financial, legal and reputational risks to the licensee and to its customers;

(d) The impact that any disruption of the activity might have on the licensee's revenue prospects; and

(e) The potential impact that a confidentiality breach or failure of data integrity could have on the licensee and its customers.

OM-2A.1 General Requirements (continued)

OM-2A.1.5 **Before entering into any cloud outsourcing arrangement, a conventional bank licensee must:**

(a) Assess if the cloud outsourcing arrangement is material;

(b) Identify and assess all relevant risks of the cloud outsourcing arrangement; and

(c) Undertake appropriate due diligence on the prospective CSP.

OM-2A.1.6 The conventional bank licensee should assess all relevant risks of the cloud outsourcing arrangement, including risks in relation to information and communication technology, information security, business continuity, legal and compliance, reputation, operations and possible oversight limitations for the licensee. These risks may arise from:

(a) The selected cloud service and the proposed deployment models;

(b) The migration and/or the implementation processes;

(c) The sensitivity of the function and the related data which are under consideration to be outsourced and the security measures which would need to be taken;

(d) The interoperability of the systems and applications of the licensee and the CSP, namely their capacity to exchange information and mutually use the information that has been exchanged;

(e) The portability of the data of the licensee, i.e. the capacity to easily transfer the its data from one CSP to another;

(f) The political stability, the security situation and the legal system of the countries where the outsourced functions would be provided and where the outsourced data would be stored;

(g) In case of sub-outsourcing, the additional risks that may arise if the sub-outsourcer is located in a different country from the CSP and, in case of a sub-outsourcing chain, any additional risk which may arise, including in relation to the absence of a direct contact between the licensee and the sub-outsourcer performing the outsourced function; and

(h) Possible concentration caused by multiple cloud outsourcing arrangements with the same CSP.

OM-2A.1.7 When assessing the suitability of the CSP, licensees should ensure that the CSP has the business reputation, skills, resources (for example human, IT and financial), and if applicable, regulatory authorisation(s) or registration(s) to perform the critical or important function in a reliable and professional manner and to meet its obligations over the duration of the cloud outsourcing arrangement. Additional factors to be considered in the due diligence on the CSP include, but are not limited to:

(a) The management of information security and the protection of personal data including periodic audit arrangements;

(b) The service support, including support plans and contacts, and incident management processes; and

(c) The business continuity and disaster recovery plans.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-2A:	Cloud Outsourcing Arrangements

OM-2A.1 General Requirements (continued)

OM-2A.1.8 Conventional bank licensees must ensure that the Board and senior management oversight and internal controls are commensurate with the the risks posed by the cloud outsourcing arrangement. In particular, licensees must:

(a) Allocate sufficient resources to oversee and manage the risks associated with its cloud outsourcing arrangements;
(b) Identify key staff and their roles for all cloud outsourcing arrangements and ensure that their knowledge and skills are kept up to date by training or other methods;
(c) Reassess the suitability of CSPs and materiality of its cloud outsourcing arrangements at regular intervals and when there are material changes to the nature, scale, complexity or risks of the cloud outsourcing arrangements; and
(d) Establish a defined escalation protocol, for both the CSP and the licensee, in respect of all its cloud outsourcing arrangements.

OM-2A.1.9 Conventional bank licensees must ensure that the respective rights and obligations of a licensee and the CSP are clearly set out in a legally enforceable written agreement. The agreement must adequately address the following at a minimum:

(a) Data confidentiality, ownership and control in compliance with CBB Law and PDPL;
(b) Information security;
(c) Data location and transfer;
(d) Licensee's and CBB's (including its appointed experts) right to access and audit the CSP;
(e) Dispute resolution;
(f) Sub-contractors;
(g) Termination; and
(h) Business continuity management and disaster recovery.

OM-2A.1 General Requirements (continued)

OM-2A.1.10 With regards to access and audit rights, conventional bank licensees can satisfy their due diligence requirements by relying on:

(a) Third-party certifications and external or internal audit reports made available by the CSP; and/or

(b) Pooled audits performed jointly with other clients of the same CSP or pooled audits performed by a third-party auditor appointed by multiple clients of the same CSP.

OM-2A.1.11 Conventional bank licensees should consider the following controls in respect of data confidentiality:

(a) Terms on confidentiality of the customer's information, documents, records, assets and online/offline backups;

(b) Logical separation of client's data where multi-tenancy and/or data commingling arrangements or practices are adopted by the CSP; and

(c) Terms on liability for losses in the event of a breach of security or confidentiality.

OM-2A.1.12 Conventional bank licensees should inform the customer on a timely basis in the event the local authorities of the jurisdiction where the data is stored are seeking or compelling the CSP to disclose the data to a third party.

OM-2A.1.13 Appendix OM-2 under Part B of the CBB Rulebook Volume 1, contains control guidelines that may be helpful to assess CSPs and cloud outsourcing arrangements.

OM-2A.2 Information Security

OM-2A.2.1 Conventional bank licensees must set information security requirements for all their cloud outsourcing arrangements in their internal policies and procedures and monitor compliance with these requirements on an ongoing basis. In this respect, the following matters must be addressed at a minimum:

(a) Ensure that the CSP complies with internationally recognised information security standards and has implemented appropriate information security controls (for example by requesting the CSP to provide evidence that it conducts relevant information security reviews);
(b) Adopt a risk-based approach to data storage and data processing locations (country or region) ensuring that the data is not stored in jurisdictions where prompt access to information by licensee or CBB representatives may be impeded by legal or administrative restrictions, or jurisdictions that are subject to United Nations sanctions.;
(c) Ensure that there is a clear allocation of information security roles and responsibilities between the licensee and the CSP, including in relation to threat detection, incident management and patch management, and ensure that the CSP is able to fulfil its role and responsibilities effectively;
(d) Ensure that strong authentication mechanisms and access controls are implemented to prevent unauthorised access to the licensee's data and back-end cloud resources;
(e) Ensure the use of encryption technologies for sensitive data including data in transit, data in memory, data at rest and data back-ups, in combination with appropriate key management solutions to limit the risk of unauthorised access to the encryption keys (for example by preventing the CSP from storing and managing encryption keys or requiring separation of duties between key management and operations); and
(f) Ensure appropriate levels of segregating networks (for example tenant isolation in the shared environment of the cloud, operational separation as regards the web, application logic, operating system, network, Data Base Management Systems (DBMS) and storage layers) and processing environments (for example development, testing, staging and production).

OM-2A.5 Information Security (Continued)

Penetration Testing and Vulnerability Assessment

OM-2A.2.2 The conventional bank licensee must ensure that the CSP conducts periodic penetration testing and vulnerability assessments. The scope of testing must encompass applications, networks and systems used to host licensee data in the cloud and address threats that are unique to cloud computing, such as hypervisor jumping and weak application programming interfaces.

Security Events Monitoring and Incident Management

OM-2A.2.3 Conventional bank licensees must identify specific cloud security incident scenarios and develop specific correlation rules to detect such events in their Security Incident and Event Monitoring (SIEM) system.

OM-2A.2.4 Conventional bank licensees must have in place procedures for the escalation, notification, containment and closure of relevant security and technology incidents and these procedures must be agreed between the licensee and the CSP. Incidents that have a material impact to the licensee must be subject to formal post incident reviews.

Business Continuity Planning

OM-2A.2.5 Conventional bank licensees must have in place cloud exit plans as part of their business continuity planning covering switching to another CSP and/or bringing the outsourced functions/services in-house.

OM-2A.3 Notification and Approval Requirements

OM-2A.3.1 Conventional bank licensees must seek the CBB's prior written approval before entering into any material cloud outsourcing arrangements. The approval request must at a minimum include the following information:

(a) A description of the outsourced functions, systems and data covering details of the business segments/lines, products and offerings, markets, geographies and operations or processes involved or impacted;

(b) Details of the CSP and any sub-contractors;

(c) Results of materiality and risk assessment of the cloud outsourcing arrangement and due diligence on the CSP; and

(d) The governance and information security arrangements that will be in place for the cloud outsourcing arrangement.

OM-2A.3.2 Conventional bank licensees must report to the CBB any material developments of cloud outsourcing arrangement including but not limited to:

(a) Any material changes in the scope of the cloud outsourcing arrangement;

(b) Data breaches or leakages detected by the licensee or the CSP;

(c) Prolonged disruption of service;

(d) Major cyber-attacks;

(e) Termination of the cloud outsourcing arrangement; and

(f) Local or foreign legal authority's request to disclose confidential data.