SUPPLEMENTARY INFORMATION
APPENDIX OM-2
Cloud Outsourcing Control Guidelines

A. Introduction

1. Cloud services enable on-demand access to a shared pool of resources such as applications, servers, storage and network. The service is deployed using various cloud models which have different inherent risks and provide for distinct operational and security trade-offs. These deployment and service models are described below:
   (a) **Software as a Service 'SaaS'** allows the use of cloud-based web applications whereby all software and hardware are provided and managed by a vendor.
   (b) **Platform as a Service 'PaaS'** refers to cloud platforms that provide runtime environments for developing, testing and managing applications without needing all the related infrastructure (servers, databases, operating systems, development tools, etc).
   (c) **Infrastructure as a Service 'IaaS'** is a cloud service that provides basic computing infrastructure: servers, storage and networking resources. IaaS services can be used for a variety of purposes, from hosting websites to analysing big data. Clients can install and use whatever operating systems and tools they like on the infrastructure they get.
   (d) **Private cloud infrastructure** is provisioned for the exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
   (e) **Community cloud infrastructure** is provisioned for exclusive use by a specific community of organizations that have shared concerns (e.g. mission, security requirements, policy or compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
   (f) **Public cloud infrastructure** is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or some combination of them. It exists on the premises of the cloud service provider.
   (g) **Hybrid cloud infrastructure** is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

2. Due to the typical characteristics of cloud services including the propensity for storage and processing to be carried out in multiple locations, controls are established to manage cloud-specific risks such as data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing.

B. Governance

1. A Board approved cloud outsourcing policy consistent with the bank's overall business and IT strategy helps comprehensively manage the bank's cloud outsourcing arrangements. Clear ownership, authority and responsibility in relation to the cloud outsourcing arrangements are defined in the policy including the involvement of business lines, IT, cyber security and other functions, as appropriate, in decision-making.

2. Key elements of outsourcing policies and procedures include:
   (a) Planning of cloud outsourcing arrangements:
      1. Business requirements regarding cloud outsourcing arrangements;
      2. The criteria and processes for identifying critical or important systems;
      3. Risk identification, assessment and management;
      4. Due diligence checks on prospective CSPs;
      5. Business continuity planning;
      6. The approval process of new cloud outsourcing arrangements;
   (b) Ongoing monitoring and assessment of the CSP's performance including notifications and changes to cloud outsourcing arrangements or CSP (e.g. related to its financial position, organisational or ownership structures, sub-outsourcing, etc.);
   (c) Information security controls;
   (d) Access and audit rights for independent review and audit;
   (e) Documentation and record-keeping; and
   (f) Exit, termination and change management processes.

3. The terms relating to resolution process, events of default, and the indemnities, remedies and recourse of the respective parties are agreed upon.

4. Dependency risk arising from the cloud outsourcing arrangements is adequately mitigated such that client remains able to conduct its business in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the CSP.

C. Data Location and Transfer

1. The following controls are agreed with respect to data location and transfer:
   (a) The client is informed where its data is stored and any changes to the location; and
   (b) The client has the right to reject any proposed change to the location of its data or terminate the cloud outsourcing arrangement on such grounds.

D. Access and Audit Rights

1. Access to CSP is not impeded or limited by contractual arrangements. If the performance of audits or the use of certain audit techniques might create a risk for another client's environment, alternative ways to provide a similar level of assurance are agreed.

2. Third-party certifications and external or internal audit reports are acceptable if:
   (a) The scope of the certifications or the audit reports covers the CSP's systems (including processes, applications, infrastructure, data centres) used to store or process the client's data;
   (b) The certifications or reports are not obsolete;
   (c) The third-party conducting the audit is qualified;
   (d) Client as the right to request the expansion of the scope of the certifications or audit reports to cover relevant controls and systems.

E. Subcontractors

1. Where sub-outsourcing is allowed the following controls are considered:
   (a) Client is informed of any sub-outsourcing;
   (b) All contractual obligations between the CSP and the client are continuously met; and
   (c) Client has the contractual right to terminate the cloud outsourcing arrangement with the CSP in case it objects to the proposed sub-outsourcing arrangement or material changes thereof.

F. Termination and Exit

1. Situations in which the client has the right to terminate the agreement include:
   (a) The CSP undergoes a change in ownership;
   (b) The CSP becomes insolvent or goes into liquidation;
   (c) The CSP goes into judicial administration;
   (d) The CSP is in breach of applicable laws, regulations or contractual provisions;
   (e) There has been a significant and material breach of security or confidentiality; and
   (f) There is a demonstrable deterioration in the ability of the CSP to perform the contracted service.

2. The minimum period to execute a termination is specified in the cloud outsourcing agreement.

3. A cloud exit plan includes the following:
   (a) Defined trigger events;
   (b) Roles and responsibilities to manage the exit; and
   (c) Alternative solutions and transition plans.

4. Data removed or transferred from the CSP is securely deleted from the systems of the CSP and, where applicable, from the systems of any sub-contractor by requesting a written confirmation from the CSP.

G. Information Security:

1. All information security risks associated with cloud outsourcing arrangements are accessed and necessary controls such as encryption, tokenisation or containerisation are implemented.

2. 'Containers' enable decoupling applications from operating systems by using a lightweight image that includes the necessities for an application at runtime. The container images contain a standard set of configurations, for both production and non-production images, that are designed and/or signed off by the client. Where containerisation is adopted for cloud hosting, roles and responsibilities between the CSP and the client are agreed upon and documented.

3. Encryption is the process of encoding messages or information in ways such that the output is rendered unintelligent. Encryption can be used to protect the confidentiality of sensitive data, provide some assurance that data has not been tampered with, and is also useful for non-repudiation. Conversely, improper design of encryption systems and processes can lead to implementations that provide a false sense of security. This can also occur when key management is weak.

4. The security of the cryptographic keys is critical to ensure that the information at rest is secure and the encrypted information is not accessible or retrievable. CSP environments typically offer a number of configurations for key management including a CSP managed option, an option to "Bring Your Own Key" where a client's key can be injected into the CSP's key management infrastructure, or an entirely client-managed option where it is possible to deploy a client-owned key management solution into the cloud.

5. The following controls are considered when implementing encryption in cloud outsourcing arrangements:
   (a) Sensitive data including data backups are subjected to appropriate encryption controls both in-motion and at-rest;
   (b) The encryption algorithms, corresponding key-lengths, data flows and processing logic are reviewed by subject matter experts;
   (c) Details on the location, ownership and management of the encryption keys and key management solution is agreed between the client and the CSP;
   (d) Key management solutions and other cryptographic material is stored on segregated secure networks where access is carefully controlled and are not accessible from subnets used by CSP's other customers or for every day staff access;

(e) Encryption keys used for the encryption of the client data are unique and not shared by other users of the cloud service;
(f) Keys are subject to rotation regularly in accordance with industry best practices;
(g) Procedures are in place for the entire lifecycle of cryptographic material from generation, storage, usage, revocation, expiration, renewal to archiving of cryptographic keys; and
(h) The cloud based key management solution meets international encryption standards.

6. In some cases, data not essential for the delivery of the cloud service is transmitted to and stored by the CSP, resulting in excessive sharing and unnecessary exposure of potentially sensitive information. Tokenisation can provide effective risk reduction benefits by minimising the amount of potentially sensitive data exposed to the public. Tokenisation is the process of replacing sensitive data with a non-sensitive equivalent value (also referred to as token) that has no correlation or meaning with the dataset. Tokenisation can be applied to all data that is not required to be processed by the CSP and is commonly used to protect sensitive information such as account numbers, phone numbers, email addresses and other personal identifiable information.

7. The following controls are considered when implementing tokenisation in a cloud outsourcing arrangement:
   (a) Careful evaluation of the tokenisation solution to identify unique characteristics and all interactions and access to sensitive data; and
   (b) The CSP has no means to restore the tokens to the original data values such as by accessing or controlling the tokenisation system or tokenisation logic.

8. Where data in transit crosses cloud deployments, content inspection technologies are deployed to identify and, where appropriate, quarantine information assets that contain personal identifiable information or customer information.

9. Where cloud services are accessible via the Internet, data loss prevention controls such as cloud access security broker are implemented to monitor and control the access of the information.

10. The 'entry' and 'exit' points are always monitored identify any used of unsanctioned cloud services or shadow IT.

H. User Access Management and Authentication

1. The life-cycle of user access management includes defining identity and access management requirements, approval, provisioning, credential management, access review and revocation.

2. A framework is created to define which system components are considered critical and what controls should be in place to manage privileged or administrative access to them.

3. The following controls are considered for access management and authentication:

   (a) Identity and access management incorporates both technical and business user access management;
   (b) A clear business owner is identified to ensure accountability and ownership of each role;
   (c) The identity and access management policies and standards are applied for production and testing environments to ensure consistency;
   (d) IP and Geo source restrictions are implemented;
   (e) User access administration is subject to strict segregation of duties and maker /checker controls;
   (f) Changes in role access rights is reviewed by an independent assurance function or the role's owner.
   (g) Where development and production environments exist in the cloud, developers, testers and quality assurance teams do not have any write access to production environments;
   (h) Multifactor authentication is implemented for user access to critical systems;
   (i) Users with privileged system access are clearly defined and subject to regular user access reviews; and
   (j) A mechanism is developed to detect any unauthorised accounts created that can access critical information assets.

I. Incident Management

1. The following controls are considered for incident management:

   (a) SLA for the escalation, notification, containment and closure of relevant security and technology incidents is created;
   (b) Material incidents are subject to formalized post incident reviews; and
   (c) Review and testing of the incident response plan conducted on a regular basis.

J. Collaborative Disaster Recovery Testing

1. Collaborative disaster recovery testing is conducted by the CSP with the client where possible. The following controls are considered:

   (a) Disaster recovery plans are developed for information assets in the cloud including recovery procedures;

(b) Disaster recovery plans are tested regularly, for example once in 2 years, and the results are validated for accuracy and completeness;
(c) Deficiencies noted during testing are recorded and corrective actions implemented; and
(d) Various disaster recovery scenarios including component failure, full site loss and partial failures are incorporated into the testing plan.