ABS Cloud Computing Implementation Guide 3.0

for the Financial Industry in Singapore

July 2024

Table of Contents

Section 1: Introduction

Objective

The Association of Banks in Singapore ("ABS") has developed the third version of the implementation guide for Financial Institutions ("FIs") to use when entering and subsequently managing cloud third-party arrangements.

The adoption of cloud can offer numerous advantages, including faster time to market, scalability, cost savings, enhanced security, and access controls. The recommendations in this guide have been discussed and agreed by the members of the ABS Standing Committee for Cyber Security ("SCCS") as industry best practices to help FIs manage the risks (e.g., multi-tenancy, data co-mingling, and data processing done in multiple jurisdictions) related to cloud third-party arrangements to support the safe adoption of cloud services. These recommendations are intended to provide general guidance to applicable regulatory guidelines and advisories and are non-mandatory.

Technology and market practices have advanced rapidly since the guide was last updated in August 2019. The Monetary Authority of Singapore ("MAS") has also issued the Advisory on Addressing the Technology and Cyber Security Risks associated with Public Cloud Adoption ("Public Cloud Advisory") in June 2021 and refreshed the Technology Risk Management Guidelines ("TRMG") in January 2021. The latest update ensures that the guide remains current to industry developments and regulatory guidelines.

This guide can also be referenced by the Cloud Service Providers ("CSPs") to better understand what is required to achieve successful Cloud third-party arrangements with FIs.

The guiding principle for cloud outsourcing arrangements is that controls in the cloud must be at least as strong as those which the FIs would have implemented had the operations been performed in-house.

These guidelines are set out in the following two sections:

- Section 2 addresses a minimum set of activities recommended for due diligence before entering into a Cloud third-party agreement.
- Section 3 addresses the minimum set of controls recommended when entering a cloud third-party arrangement.

Note

- General outsourcing related recommendation and guidance have been removed from v3.0 and the focus will be on the best practices unique to cloud outsourcing. FIs should refer to the relevant MAS Notices and Guidelines on Outsourcing for details on general outsourcing requirements.
- Not all activities and controls in section 2 and 3 are applicable to all types of service models. FI should review and apply where applicable.

Cloud Computing Models

The definition of cloud computing and cloud deployment models referenced are from the National Institute of Standards and Technology ("NIST") Special Publication 800-145 – The NIST Definition of Cloud Computing published in 2011.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of three service models, and four deployment models.

Community cloud
cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection

Hybrid cloud
cloud deployment model that uses a private cloud and a public cloud

Private cloud
cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer

Public cloud
cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider

Multicloud
cloud deployment model in which a cloud service customer uses public cloud services provided by two or more cloud service providers

[1]**Service models (IaaS/PaaS/SaaS).** There could be [2]nuances in the shared responsibility model within the three commonly known service models to consider (e.g., CSPs manages the security of the Key Management System while FIs manages the security of key generation and transportation in a Bring-Your-Own-Key ("BYOK") arrangement.

[3]**Deployment models ([4]Public, Private, Hybrid, Community).** That there could be various terminology (e.g., dedicated cloud, virtual private cloud) used by commercial Cloud Service Providers (CSPs) with regards to deployment models. It is important for FIs to understand the underlying setup when implementing cloud to select the appropriate deployment model for their workload. The following factors may be considered when determining the deployment model. FIs should consider the factors below when deciding the appropriate deployment model for their cloud implementation.

(i) **Single tenancy versus multi-tenancy.** FIs may review the supplier service contract to discern the tenancy arrangement and if there are any shared components when classifying the deployment model of the cloud service.

[1] Refer to Appendix A1 for Service Models described in the NIST Special Publication 800-145
[2] Footnote 4 and Diagram 2 in the MAS Public Cloud Advisory provides further guidance on Service Models.
[3] Refer to Appendix A2 for Deployment Models described in the NIST Special Publication 800-145
[4] Note that MAS has also described Public Cloud Services as "a combination of a business and delivery model that enables on-demand, public access to a shared pool of resources such as applications, servers, storage and network security" in footnote 2 of the Public Cloud Advisory; as well as "a cloud infrastructure made available to the general public or an industry group, and is owned by a third party service provider" in footnote 28 of the Guidelines on Outsourcing.

(ii) **Hosted private versus on-premise managed private cloud.** The shared responsibility model may differ between a hosted private cloud and an on-premise managed private cloud. While a CSP may deploy and provide managed service of the private cloud infrastructure at the premises of the FI for its exclusive use, the FI may continue to assume responsibility for the environmental and physical security controls. For on-premise services, the FI may continue to reference controls in this Guideline where appropriate.

(iii) **Dedicated versus non-dedicated**. It is important for FIs to understand the extent of what is considered dedicated resources when determining the deployment model. It is possible that a "dedicated cloud" refers to dedicated network or compute resources, but not the physical host.

Section 2: Cloud Risk Assessment & Due Diligence

This section covers the recommended risk assessment and due diligence activities for cloud third-party arrangements on top of general outsourcing and third-party risk management. For details on general outsourcing requirements, FIs should refer to the relevant MAS Notices and Guidelines on Outsourcing. FIs can also refer to Section A 3.3 in the MAS Operational Risk Management – Management of Third-Party Arrangements Information Paper[5] on good practices related to third party risk management that the MAS expects to see in banks.

The recommendations below will cover both pre-engagement of the CSP and post-implementation on-going risk assessment and oversight. FIs should use a risk-based approach and an applicability assessment to determine the relevance of the recommended activities for their specific outsourcing arrangement.

1. Cloud Governance

It is paramount that governance structure is in place to manage cloud outsourcing and cloud implementation in general. Cloud outsourcing may continue to be managed within the existing outsourcing governance framework. In addition, it is recommended that cloud strategy and cloud governance be integrated in the FI's IT governance and risk management framework to ensure alignment to the overall IT strategy and risk appetite.

Concentration Risk Management - FIs are recommended to build on existing third-party and outsourcing risk management process to ensure that CSP concentration risk can be identified and managed effectively. This may include enhancing the process to:

- Maintain inventory of CSP exposures across various IaaS/PaaS/SaaS third party arrangements to provide a holistic view on dependency of a single CSP (including CSPs as sub-contractors of SaaS outsourcing.
- Assess concentration risk at CSP level (including CSPs as sub-contractors of SaaS outsourcing). Such risk evaluation to be re-performed periodically or when proposed new cloud outsourcing relates to the same CSP.
- Maintain inventory of CSP specific availability zone ("AZ") exposures for IaaS/PaaS workloads and SaaS to provide holistic business impact analysis for any potential AZ failure/ outage.

2. Cloud Third-Party Arrangement Due Diligence

FIs should ensure that existing risk management framework and third-party due diligence process can address the risks associated with the use of cloud and CSPs and their material sub-contracting arrangements.

Pre and Post Implementation Reviews - FIs should establish their own third-party risk management framework and the necessary policies and procedures that are commensurate with the materiality of the arrangement for the scope of their pre- and post-implementation reviews.

Besides due diligence on the CSP, pre-implementation reviews should include checks and controls to ensure a smooth handover of the functions from FIs and/or other service providers to the new service providers. Post-implementation reviews may include reviewing the effectiveness and adequacy of the FIs' controls for monitoring the performance of the service provider and checks to

[5] https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2022/operational-risk-management---management-of-third-party-arrangements.pdf

ensure that the risks associated with the activity are managed appropriately as planned. Post-implementation reviews are usually conducted shortly after the commencement of the cloud arrangement. The MAS expects FIs to determine an appropriate frequency for these post-implementation reviews.

Contractual Agreement - When negotiating a contract with a CSP, the FI should ensure that it can contractually enforce agreed and measurable information security and operational requirements. Without such authority, any control put in place for the cloud third-party arrangement may not be enforced, as the FI will be relying on good faith of the CSP. FIs should comply with the MAS Outsourcing Guidelines when negotiating and drafting of the outsourcing agreement. Additionally, FIs may refer to the following guidance for cloud third-party arrangements:

Service Level Agreements - Enforceable and measurable Service Level Agreements (SLAs) should be negotiated where possible, particularly for material outsourcing arrangements. These should include defining the governance structure to be put in place to manage the contract on an on-going basis. This should define any management information and other deliverables that will form the basis for that governance. FIs should be aware of composite SLAs and ensure they meet their overall requirements. Where SLAs are negotiated, these must be aligned with business requirements and where possible, appropriate contractual remedies or enforceable liquidated damages clauses are included.

FI should understand and agree with the CSP on the change management process for the services provided and the impact assessment criterions for the SLA in the contract. The FI should ensure that the outsourcing agreement includes an obligation for the CSP to notify the FI of any significant changes that may impact the security or service availability (including controls and/or location).

Key Indicators ("KIs") - Once responsibilities are understood and agreed, appropriate KIs (including Key Performance Indicators, Key Risk Indicators, Key Control Indicators), key activities, inputs and outputs should be defined in the SLA. The governance of the SLA and the tools recommended for the tracking should also be defined in the service agreement. KIs should indicate the effectiveness of key controls, which are subject to periodic review. The control testing interval should be determined by the FI based on a risk-based approach.

Asset Classification. The FI should have a clear policy on the classification of the assets that are outsourced to CSP. Such policy should include the FI's ability to assess and determine the controls necessary for protecting the data confidentiality and integrity and the location where the data should be hosted.

Data Confidentiality and Control ownership - The FI should ensure that the third-party service agreement includes the following requirements:

(a) Ensure the CSP can protect the confidentiality and integrity of FI's information, documents, records and assets, particularly where multi-tenancy and/or data commingling arrangements or practices are adopted by the CSP.

(b) If the service agreement with the CSP terminates on expiry or prematurely, the FI has the contractual right to promptly render data inaccessible at the CSP's systems (including backups)

(c) Provision to address specific regulatory requirements, such as the right to audit by the MAS and prompt notification of security incidents or technology outages that have a material impact, must also be included in the outsourcing agreement if relevant.

Data Retention - FI must be able to stipulate access to all its data including those used for daily operational purposes and for contingency, disaster recovery or backups.

An area of concern would be the management of data in online or offline backups. Where data can

be isolated or logically segregated this is simpler to manage. However, in a shared environment, the FI should ensure it has assessed that its data is protected by verified and appropriate technical means as part of the due diligence process.

For encrypted data, FI should ensure that the appropriate cryptographic key management is in place and validate the CSP's ability to restore the service from backups effectively.

Upon exiting a contract with a CSP where the FI does not have direct access to its data, FI should ensure that the CSP covers the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls are tested. This is for the CSP to assure the FI that after the exit of the service agreement, its data is rendered permanently inaccessible in a timely manner, including any backup, or distributed online media.

Cross-Border Data Transfers and Location of Data - The FI should consider the social, political, and economic climate of a jurisdiction before an FI agrees to have its data stored or processed there. FIs should at the outset obtain legal advice to ascertain that the CSP is operating in jurisdictions that generally uphold confidentiality clauses and agreement. An FI should enter into outsourcing arrangements only with CSPs operating in jurisdictions that generally uphold confidentiality clauses and agreements.

Where the FI does not control the location of its data, the FI and CSP should agree where the FI's data can reside, especially which countries or states if there are differences between the jurisdiction of federal and state courts. (For example, in federations like the United States, areas of jurisdiction apply to local, state, and federal levels.). A contractual clause requiring advance notification by the CSP of any changes to these locations should be included in the service agreement. Where the FI does not have the contractual right to reject any proposed change to the location of its data, it is recommended that the FI should retain a right to terminate the outsourcing agreement in the event of an unsatisfactory change or new location.

To ensure that data remains protected even if it leaves the jurisdiction of Singapore, unless prohibited by applicable laws, it is recommended that FIs establish contractually binding requirements that require the CSP to notify the FI if the local legal requirements compel the CSP to disclose the data to a third-party, bearing in mind section 47 of the Singapore Banking Act.

An FI should not enter outsourcing or cloud third-party arrangements with CSP in jurisdictions where prompt access to information by the MAS or agents appointed by MAS to act on its behalf, may be impeded by legal or administrative restrictions at the CSP.

Audit and Inspection - CSP should provide reasonable access to necessary information to assist in any FI investigation arising from an incident in the cloud or audit inspection, to the extent that it is does not contravene any other legal obligations. FIs should follow up with the CSP to ensure that all appropriate and timely remediation actions are taken to address any audit finding.

FI should also consider the availability of support from a CSP during an audit, including resources, costs and turn-around times for requests for information.

Business Continuity Management - FI should evaluate and validate that the interdependency risk from the arrangement can be adequately mitigated to allow the FI to conduct its business with integrity and competence during a service disruption or unexpected termination of the arrangement or liquidation of the CSP. These should include taking the following steps:

(a) Prior to contracting with the CSP, verify that the CSP has satisfactory business continuity plans ("BCP") and can recover the outsourced systems and/or IT services within the stipulated Recovery Time Objective ("RTO").
(b) Proactively seek assurance on the state of BCP preparedness of the CSP or participate in joint testing of the outsourced services (such as SaaS or PaaS) where possible. FIs should

ensure the CSP and FI regularly test its BCP and that the tests validate the feasibility of the RTO, Recovery Point Objective ("RPO") and resumption operating capacities; and

(c) Ensure that plans and procedures are in place to address adverse conditions or termination of the outsourcing arrangement to allow the FI to continue business operations. All documents, records of transactions and information previously given to the CSP should be promptly removed from the possession of the CSP or deleted, destroyed, or rendered unusable.

Third Party Risk Management - The CSP should be able to demonstrate that it implements and maintains a robust risk management and governance framework that effectively manages the cloud service arrangements including any sub-contracting arrangements.

Subcontractors - Where a CSP elects to use subcontractors to perform the services which have a material impact to the provision of the cloud service, the FI and the CSP should agree on an appropriate notification method for changes in material subcontracting for the FI to exercise oversight. The CSP remains primarily accountable to the FI for the provision of service and effectiveness of agreed controls including IT security and contractor on-boarding controls. The service agreement should include clauses making the CSP contractually liable for the performance and risk management of its sub-contractor. The CSP should also be accountable for managing their subcontractors and remediating any non-performance issues identified. Where the FI does not have the contractual right to reject any proposed subcontractor, the FI should retain a right to terminate the service agreement in the event of an unsatisfactory performance of the subcontractors, or if the subcontractor is or has become prohibited by the regulator. Access to FI data by subcontractors should require appropriate risk assessment of the subcontractor environment and processes.

Default Termination - Refer to the MAS outsourcing guidelines for details on default termination and early exit.

Exit Plan - The extent of exit planning should depend on the materiality of the outsourcing arrangement and potential impact to the on-going operations of the FI and consider the following:

1. Agreed procedure and tools used for deletion of data from CSP's environment to render the data irrecoverable.
2. Costs associated with the exfiltration and return of an FI's data.
3. Removal of all FI's data (e.g., customer data) and confirmation that all data has been rendered irrecoverable on termination of the outsourcing arrangement.
4. Transferability of outsourced services (e.g., to a third party or back to the FI) for ensuring service continuity.

For recovery of data for ensuring service continuity, FIs should ensure the following are in place where appropriate:

1. A legal agreement that commits the CSP to assist in the exit process so as not to unreasonably impede the exit or the testing of an exit plan. These should include the format and the way data is to be returned to the FI and the support from the CSP to ensure the accessibility of the data.
2. FI and CSP should agree on the data elements to be extracted and returned to the FI before entering the outsourcing arrangement and review the scope if there are material changes to the arrangement.

Shared Responsibility - The CSP and the FI should agree on the operational contract management, SLA management, technology risk management, business continuity management and contract exit. CSPs should provide assurance to FIs that there is stringent governance on their

daily operational procedures and is validated via independent assurance process. (Refer to the MAS Cloud Advisory for example of a Shared Responsibility Model)

The FI should ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements.

Moving technology infrastructure into the cloud creates a shared responsibility model between the FI and the CSP for the operation and management of security controls. According to MAS's Cloud Advisory, CSPs are responsible for "Security-of-the-Cloud"[6], FIs would be responsible for "Security-in-the-Cloud"[7].

FIs should assess and have a clear understanding of the shared cyber security responsibilities based on the different Cloud Service Model being adopted.

FI should perform due diligence to understand the services they are adopting and what their CSPs responsibilities are. The delineation of responsibilities differs according to the type of services subscribed from the CSP. FIs should reference known international cloud standards published by the Cloud Security Alliance ("CSA") and NIST.

Below are examples where these delineations require further diligence and deliberation on what the FI and CSP is responsible for. For example,

- Privileged User Management. The responsibility of providing the access management and securing access to the native service would be provided by the CSP but the configuration of permitted users would be the responsibility of the FI.
- Disaster Recovery Testing. FI can perform testing on their end on the application layer but require the support of the CSP to perform a full disaster recovery testing. Often, it may also not be feasible due to the nature of a multi-tenancy environment.
- Network Security. Although generally provided by the CSP who owns the underlying infrastructure and have direct access, FI is responsible to ensure encryption or permitted accessibility between endpoints in the cloud.
- General Misconfiguration of Services. FIs usually have some capabilities to configure their services and need to periodically review the configurations to ensure best practices are applied to prevent commonly seen cloud security breaches.

[6] "Security-of-the-Cloud" refers to the security of the public cloud services under the CSPs' responsibility. In an IaaS or PaaS arrangement, these would typically include the security of the underlying hardware, system software and the hypervisor. For SaaS, this would also include the underlying security of the application software.
[7] "Security-in-the-Cloud" refers to the security of the cloud workloads under the FIs' responsibility. In an IaaS or PaaS arrangement, these should typically include securing IT systems components such as applications, operating system and orchestration tools. In a SaaS arrangement, it would generally include managing user account privileges and data access rights.

Section 3: Key controls recommended when entering into a cloud outsourcing arrangement

This section recommends the baseline security controls for implementation of cloud workloads which should be applied according to the criticality of the cloud workload.

The Journey to the Cloud

A. Govern the Cloud (setup and on-going management) • Organisational Considerations for the Management of CSPs • Control Assessment & Monitoring • Billing Models
B. Design and Secure the Cloud (pre-implementation) • Cloud Architectural Reference Solutions & Practices • Virtualisation, Containerisation and DevOps • Resiliency in Cloud Architectures • Network Architectures • Cryptographic Key Management • Encryption • Tokenisation • Authentication & User Access Management • Privileged User Access Management (PUAM) • Administrative Remote Access • Data Loss Prevention • Source Code Reviews • Penetration Testing • Security Events Monitoring • Securing Logs and Backup
C. Run the Cloud (on-going basis) • Change Management • Configuration Management • Events Management • Incident & Problem Management • Capacity Management • Patching and Vulnerability Management • Collaborative Disaster Recovery Testing

A) Govern the Cloud

1. Organisational Considerations for the Management of Cloud Service Providers

FIs scaling their technology footprint through cloud adoption should consider adapting their organisational structure to ensure effective and timely oversight of CSPs for their performance, operational effectiveness of controls and remediation.

Control Objectives

- Ensure there is accountability and governance in place that bridges the FI and CSPs
- Execute robust and timely oversight of risks associated with cloud outsourcing arrangements.
- Ensure that FI has the appropriate skills and knowledge to execute oversight and manage cloud operations on a continuous basis.
- Have an integrated, consistent, reliable, and empowered management and escalation interface between FI's business and operations divisions and the CSPs to ensure service delivery, security management and incident management.

Considerations of Controls

1. Based on the model of shared responsibility defined during the contractual negotiations, an FI should design and implement a suitable governance forum and roles with appropriate representatives from both the CSP and the FI. The governance forum should be empowered to oversee adherence to SLAs, review KPIs and KRIs, operations (cloud health), finance (costing, penalties, saves), operational incidents (e.g., outages, degradation), security incidents, developer experience (self-service, ease of use), skills uplift (trainings) and other relevant matters to the risks associated with outsourcing. This governance forum should meet periodically, the frequency determined by the materiality of the arrangement.
2. Based on the service outsourced, governance forum should have appropriate representation from technology and business of the FI and a single point of contact from CSP.
3. A defined escalation procedure should be put in place for both CSP and FI to use.
4. It is recommended that KPI and KRI metrics be defined for governance to provide a complete view of the controls that are owned and operated by the FI or the CSP. FIs should consider interfaces to internal governance bodies for FI-owned controls.
5. FIs may consider creating/appointing a specific role to execute oversight of cloud third-party arrangement(s).
6. Execution of oversight of cloud outsourcing arrangements requires specific skillsets. FIs should identify key staff and roles and ensure that their knowledge is kept up to date by training or other methods.
7. When performing due diligence activities, or during audits and regulatory inspections it is recommended to use appointed individuals and a central point to coordinate activities between the CSP, FI and the auditor.
8. Any incremental changes to outsourcing controls should be managed via the governance forum.
9. If using a multi-cloud strategy, the governance forum should maintain a consolidated view of all CSPs to facilitate a holistic view of any potential concentration risk and increase workload portability.

2. Control Assessment & Monitoring

The FI should establish an appropriate control framework to manage the risks associated with the intended workloads and define the controls to meet corporate policies and regulatory. Where possible, control testing should be automated and tested at a frequency determined by the FI’s risk appetite.

Risk assessment should assess the general security of the CSP and specific services to ensure required controls are implemented and operating within acceptable thresholds.

Control Objectives

- Demonstrate compliance position against regulatory requirements, corporate policies, and standards.
- Regularly test key controls to provide assurance of the design and operational effectiveness of the overall control framework.
- Where non-compliance is detected trigger an appropriate and timely response for remediation

Considerations of Controls

1. Prior to embarking on any cloud third-party arrangement, FIs should perform a thorough risk assessment of key controls on the use cases.
2. Establish management information and dashboard material for reporting on control assessments. Define an appropriate oversight model for communication, decision making and escalation to execute remediation activities which considers both FI and CSP-owned activities.
3. FI should consider leveraging the controls available in the cloud environment to enforce consistent security standards and baselines and automate remediation where possible.
4. FI should consider the use of data analytics and other best in breed technologies to develop baselines for compliance checks to highlight and avoid non- compliance.
5. Where possible an FI should ensure that a control failure triggers an automated response and notification.

3. Cost Management

Strategic adoption of cloud is usually supported by a business case. With a distributed model of consumption, FI should track usage to ensure clear ownership of costs and facilitate internal distribution of these expenses.

Control Objectives

- Ensure clear ownership of cloud usage costs.
- Ensure that excessive or unnecessary usage is prevented or identified and managed timely.
- Facilitate transparency in overall cloud usage for management information and strategic decision making.

Considerations of Controls

1. It is recommended that the FI maintain a centralized governance structure to manage master subscription and control how that is provisioned for specific workloads.
2. Identify and assign clear ownership for all assets in the cloud and assign the asset classification.
3. Do not use the CSP's master account to centrally manage the costs, create sub accounts for consuming units which are aligned and tracible to the financial reporting and budgeting structure of the FI.
4. Provide tailored training and educational resources for users of the cloud environment to help them understand the best adoption methods and use of cloud resources efficiently.
5. Work with CSPs to create usage reports at regular intervals which are made available to account owners and for presentation to appropriate governance forums. Ensure that these reports are consumed in line with technology financials and internal billing standards.
6. Define quotas for each sub account and put in place alerts or triggers once a threshold of spending has been reached.

7. Include all relevant cloud stack components, software licensing, compute, storage, and network costs in the cloud usage reporting,
8. Maintain sufficient funds to cover licensing costs and that controls are in place to prevent key services being shut down in case of license expiration or capacity issue.
9. Formally agree protocols with the CSP to prevent cessation of services due to oversubscription of cloud resources.

B) Design and Secure the Cloud

1. Cloud Architectural Reference Solutions & Practices

As CSPs allow FIs to host their workloads in their cloud environment with a myriad of options to cater for diverse workloads and needs and due to the foreign nature of the cloud environment, initial attempts to adopt the cloud services can be daunting. Many CSPs have developed cloud architecture reference solutions to solve common cloud adoption problems to help customer jumpstart their cloud implementation.

As cloud service consumption is commoditized, it is important to architect a standard catalogue of services which adhere to the business, technology and security standards of the FI.

Control Objectives

- Design and implement cloud services which are optimized to create the largest financial and non-financial benefits to the FI.
- Create a service catalogue of cloud products that adhere to the FI's internal policies and regulatory requirements.

Considerations for Controls

1. FI should adapt the existing technology architecture governance to set standards and approve cloud patterns but leverage the CSP expertise for cloud design patterns.
2. FIs should review business and technology requirements when developing cloud reference architectures by publishing and periodically reviewing the Business Requirement Documents (BRDs) and System Requirement Documents (SRDs).
3. FI should have an appropriate approval workflow if end users are allowed to deploy cloud computing services or workloads directly.
4. FI should enforce strict control of access rights over creation of non-standard architectures.
5. FIs may consider adopting the commonly available architectural references for availability and resiliency, security, authentication, performance, operations and management.
6. FI should have a holistic understanding of the cloud environment and architecture and the accompanying risks associated with cloud connectivity, logical segregation and public access when considering the security architecture deployment in the cloud.

2. Virtualisation, Containerisation and DevOps

As cloud is a distributed environment, the management of the underlying software images, containers and approach to release management is a key consideration when architecting a cloud solution.

CSPs will usually provide segregation via logical controls in a virtual environment. FI should consider performing risk assessment with additional controls such as encryption or tokenisation.

In certain circumstances, such segregation may be bypassed or during a system failure, data could be accessed by exploiting data dumps and accessing infrastructure shared memory.
Operational complexity of virtual architectural models can also result in a weakened security model.

To assist in development of cloud infrastructure, FIs should assess the level of maturity, information and support available to assist with virtual architectural models; and consider potential compromise of hardware, Operating System (OS) images or virtualisation management software such as hypervisors.

The traditional virtual machine is not the only option available to FIs to host their workloads. Containers enable FIs to decouple applications from operating systems by using a lightweight image that includes the necessities for an application at runtime. These can include binaries, libraries, and settings. The ability to decouple the application from the operating system allows FIs to focus purely on managing the application. CSPs also offer serverless option to FIs to dynamically manage the allocation of systems to the workload processing requirements. These new offerings and DevOps allow FIs to easily automate the administration of their cloud environment.

DevOps and DevSecOps are hybrid approaches towards development, security and operations that have become relatively mainstream and FIs should determine the appropriate tools for DevOps and DevSecOps.

Control Objectives

- Manage the confidentiality and integrity risks associated with data co-mingling or shared tenancy environments.
- If a software or hardware fails, ensure that information assets remain secure or are securely removed.
- Define a standard set of tools and processes to manage containers, images and release management.

Considerations for Controls

1. FI should define a standard for containerization and DevOps methodologies. While the CSP may provide the tools for the FIs to manage and administer containers, the FIs are responsible for authorizing which ones are available for use.
2. FI should agree on and document the roles and responsibilities between the CSP and FI for the container strategy must be agreed upon and documented for operational references. Ensure that source code repositories are defined and managed at both the FI and CSP. If the source code repository is hosted at the FI, the binaries should be compiled on premise and only the source code artefacts need to be promoted and sent to the CSP.
3. FI should carefully define its user access and authentication strategy, particularly for administrative users who can manage and change these fundamental tools supporting its cloud ecosystem.
4. The container images should contain a standard set of configurations that are designed according to the industry best practices and approved by the FI. Standards should be created for both production and non-production images.
5. The ability to add security and vulnerability patching where applicable to the containers and virtual machine are done to the base image in a controlled manner and adheres to the standard change management process.
6. FI change management process should adequately support the dynamic nature of containerized workloads such as scaling, on-demand deployments, blue/green versions, etc.
7. Any changes to the container base images are logged and auditable.
8. FI should consider ensuring container images are immutable post approval for production deployment.
9. The CI/CD pipeline should be configured to perform the correct actions and activities against the designated environments. This could be to both containers and virtual machines.
10. Align any code deployment and configuration changes to the FIs change management

process.

11. Integrity checks should be performed on container templates and any inconsistencies made detectable prior to use.
12. FIs should have the appropriate checks to prevent production data being used during testing in non-production environments and use masked or synthetic data.

3. Resiliency in Cloud Architectures

Cloud services providers design the architecture of their cloud services to offer high resiliency and availability to their customers. In most set ups, the computing capacity of two or more data centers are grouped into a cluster and multiple clusters are further grouped into a region to achieve the resiliency and availability objectives. Each cluster is geographically separated by a physical distance to avoid systemic failure due to environmental hazards such as power outages, fires, floods etc. Fault isolation is further implemented within each region to prevent the risk of contagion effect during a fault or service outage.

Customers of the cloud services can choose to distribute their workload across multiple regions to reduce latency for their users or mitigate against regional outage of the cloud services. However, customers can also choose to constrain their workload to a single region or cluster. This allows customers with specific requirements such as data sovereignty to control the residency of their data. FIs should be cognizant that such a design potentially negates the resiliency and availability offered by cloud services.

Hence, FIs need to carefully consider and plan their cloud adoption to ensure that the resiliency and availability of the cloud services commensurate with their needs.

Control Objectives

- Ensure that the resiliency, recoverability, and availability design of the workload is commensurate with its criticality.

Considerations for Controls

1. FIs could maximize the redundancy by designing and distributing their production workloads across the available clusters within each region.
2. FIs should implement automated health checks and monitoring to detect service faults or outages in the cloud environment.
3. Where possible, FIs should design their workload and applications to automatically handle known exceptions or failures to ensure their cloud service can recover swiftly in an event of an incident.
4. FIs should design their workload to leverage on available functionalities such as containerization, auto-scaling and load balancing to automate the swift recovery of their services.
5. FIs should also adopt fault tolerant techniques such as Retry, Circuit Breakers and Bulkhead Isolation in their design of their workload which are sensitive to faults or failures.
6. For workloads that are sensitive to latency, FIs should implement the workload in the region that is closest to the users or consider options to optimize user experience (such as content delivery networks).
7. For workloads that require higher availability, FIs can consider distributing the workload across multiple regions. At minimum, the FIs should make plans to recover their services in a different region to mitigate against the regional service outages.
8. While data within each region is automatically replicated across the available clusters, FIs should consider strategies for replicating data across regions to ensure data availability in an event of failures or service faults within each region. Cross border regulatory requirements

should be considered when replicating data across regions.

9. FIs should put in place a recovery plan for its critical services in an event of a total outage of cloud services. Some of the options that the FI could consider include implementing critical workload on two different CSPs or retention of on-premise capabilities for added resiliency. Resiliency assessment should be performed before implementing multi-cloud option to ensure that it will enhance the resiliency of specific critical workload.
10. FIs may develop a methodology to assess its own cloud concentration risk and identify possible mitigating measures, such as building redundancies, deploying on multiple geographic regions, deploying a multi-cloud strategy However, FIs should be cognizant of the added complexity of operating in a multi-cloud environment, such as having adequate resources and appropriate expertise in securing and managing the use of different public cloud services and ensuring the consistent enforcement of policies.
11. FIs using multiple public cloud services may need to centrally manage security policies over the use of different public cloud services and ensure that the policies are consistently enforced.

4. Network Architectures

Network architecture is a key consideration especially due to the open access and shared services of public cloud. FI should plan and implement security controls to secure the cloud workload against common internet-based attacks (e.g., network intrusion attempts, DDoS attacks) and cloud-specific attacks.

Control Objectives

- Reduce contagion risk between the FI's on premise and cloud environment.
- Ensure access to the cloud environment are granted on a need-to basis.
- Ensure that cloud workload is protected against network-based attacks e.g., network intrusion attempts, application and DDoS attacks.

Considerations for Controls

1. FI should implement measures to secure the cloud and on-premise environments to mitigate contagion risks. Controls should be implemented between the cloud and the FI's on premise environment and at the ingress/egress points to mitigate against such threats.
2. FI should segregate the administrative interfaces in a management network that is inaccessible from the operational subnets.
3. FI should implement network access and security controls such as firewalls, IPS, advance threat protection and web proxy to secure the on-premise environment from the cloud.
4. FI should have network access and advance threat protection controls implemented in the security network segment to filter and secure access to the cloud environment.
5. FI should implement site-to-site VPN or direct network connection to secure the traffic between the cloud and on-premise environments where possible and consider IP source and destination restrictions.
6. FI should monitor and control the access, where possible, to their cloud environment.
7. FIs should implement an internal monitoring control to detect the unauthorized adoption of cloud services.
8. FI should consider network segregation of workloads based on their type (production, test, development) and purpose (user, server, interface, critical infrastructure segments).
9. While most CSPs will provide network layer DDoS attack protection, FIs should consider the implementation of application layer DDoS attack protection and web application firewall to secure the cloud-based application as required.
10. FIs should regularly review firewall rules and access lists, especially after network or architectural changes that may make certain rules redundant. Rulesets should have defined

owners.

11. FIs should implement dedicated network connectivity from the FI to the cloud environment and restrict remote administrator access to the cloud environment over the Internet.
12. The controls in the cloud environment should be equivalent if not more secure than the FI's on premise environment. Alternatively, FIs can reroute the cloud traffic through the FIs' on- premise environment to benefit from their existing on-premise security controls.
13. FI should set up a dedicated security network segment to control all ingress and egress traffic from the cloud environment.
14. FI should consider micro segmentation with software defined networks.
15. FIs should route all internet traffic through a dedicated security network segment and restrict direct access to the Internet for all other network segments in the cloud environment.

5. Cryptographic Key Management

The cloud environment leverages on the cryptographic controls to control access, and segregate and secure the customers' data. The security of the cryptographic keys is critical to ensure that the confidentiality and integrity of sensitive data in the public cloud are secure and the encrypted information, especially archival information, are retrievable.

CSP environments typically offer several configurations for key management including a CSP managed option, an option to "Bring Your Own Key" where an FI's key can be injected into the CSP's key management system, Hardware Security Module (HSM) infrastructure, or an entirely FI-managed option where it is possible to deploy an FI owned HSM into the cloud.

These deployment offer advantages and disadvantages: in the case of FI-owned and deployed HSMs this typically means that the cloud environment can only be managed and operated by the FI. Thus, it is less suitable for PaaS or SaaS environments, and can restrict the adoption of cloud services.

Furthermore, if keys are compromised or lost, the entire cloud environment may become inaccessible but this model provides the highest level of control for the FI over the cloud environment.

Control Objectives

- Manage cryptographic material so that the confidentiality and integrity of the FI's data is not compromised.

Considerations for Controls

1. Rotate keys regularly in accordance with the industry best practices. Test certificate revocation according to industry best practices.
2. Implement detailed policies and procedures to govern the lifecycle of cryptographic material from generation, storage, usage, revocation, expiration, renewal, types of keys used to archival of cryptographic keys.
3. Implement backup of cryptographic material and ensure that the keys cannot be compromised and are subject to strict oversight and segregation of duties principles. No one key custodian should have access to the entire key.
4. Generate FIs' own unique cryptographic keys and secure the keys in the cloud environment.
5. At minimum, the cloud based HSM should meet the FIPS or Common Criteria for cryptographic products. Leverage on a FIPS 140-2 Level 2 validated HSMs at a minimum to secure their cryptographic keys, and access to the HSM should be secured with multi-factor authentication. Dual authorization can be used to prevent lockout.[8] Some tools allow the access to be split among more than two people (e.g., Quorum).

[8] Dual Authorization. NIST Glossary. Source: https://csrc.nist.gov/glossary/term/dual_authorization

6. Store the encryption keys separately from virtual images and information assets, where feasible.
7. Implement carefully designed processes including appropriate key ceremonies if cryptographic keys and TLS private key of the FI are loaded into the CSP environment.
8. Implement suitably secure and fireproof environment for offline storage of critical cryptographic material as any loss may materially impact the FI's ability to recover data or operate. This should be included in disaster recovery planning scenarios.

6. Encryption

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. Conversely, improper design of encryption systems and processes or weak key management may provide a false sense of security.

Encryption can be applied in most cloud computing use cases and should be an integral control to secure sensitive information such as authentication credentials, personally identifiable information, credit card information, financial information, emails and computer source code.

CSP environments typically offer several configurations for key management including a CSP managed option, an option to "Bring Your Own Key" where an FI's key can be injected into the CSP Hardware Security Module (HSM) infrastructure, or an entirely FI managed option where it is possible to deploy an FI owned HSM into the cloud.

These deployment options offer advantages and disadvantages: FI-owned and deployed HSMs this typically means that the cloud environment can only be managed and operated by the FI. Thus, it is less suitable for PaaS or SaaS environments and can restrict the adoption of cloud services. There is also an associated cost, and if keys are lost, all data in the cloud maybe unrecoverable.

CSPs will usually provide segregation via logical controls in a virtual environment, an FI should risk assess these in combination with other controls such as encryption or tokenisation.

Control Objectives:

- Provide assurance that only authorized parties can gain access to the data in transit and at rest.
- Provide assurance that the confidentiality and/or integrity of the data has not been compromised.
- Provide authentication of source and non-repudiation of message

Considerations for Controls

The FI should ensure that the following controls are considered when implementing encryption in cloud outsourcing arrangement:

1. Sensitive data including data backups should be subjected to appropriate encryption controls both in-motion and at-rest.
2. Details on the encryption algorithms, corresponding key-lengths, data flows, and processing logic should be appropriately reviewed by subject matter experts to identify potential weaknesses and points of exposure.
3. HSMs and other cryptographic material including those used by key management should be stored on segregated secure networks where access is carefully controlled and are not accessible from subnets used by CSP's other customers or for administrative / operations staff access where applicable according to the shared security responsibility model.
4. Encryption keys used for the encryption of FI data should be unique and not shared by other users of the cloud service.

5. Other guidance on encryption requirements can be drawn from the MAS Technology Risk Management Guidelines or NIST Key Management Guideline[9].
6. Stringent control should be exercised over cryptographic keys to ensure that encryption keys are generated and managed securely, for instance within a Hardware Security Module (HSM).
7. Details on the location, ownership and management of the encryption keys and HSM should be agreed between the FI and the CSP. The FI should take into consideration the need and ability to administer the cryptographic keys and the HSMs themselves.
8. If using a Content Delivery Network (CDNs) ensure there are appropriate controls in place for encryption key and certificate management and use Extended Validation (EV) or Organisation Validation (OV) certificates to ensure robust organisational identity controls are in place. Secure certificate management protocols should also be considered.
9. Carefully designed processes including appropriate key ceremonies should be in place if cryptographic keys and SSL private key containers belonging to the FI need to be introduced into the CSP environment.
10. Include metrics for tracking compliance of encryption according to applicable risk levels and encryption standards.

7. Tokenisation

Cloud computing generally involves the transmission of data to the CSP for processing or storage. 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.

FIs should minimise its data footprint to reduce the vulnerability surface and potential threat vectors. 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 the sensitive data with a non-sensitive equivalent value (also referred to as token) that has no correlation or meaning with the dataset and the token used should be randomized whenever possible. A tokenised dataset retains structural compatibility with the processing system and allows the data to be processed without any context or knowledge of the sensitive data, thereby potentially allowing a different set of security requirements to be imposed on the recipient of the tokenised data. The FI can de-tokenise and restore context to the processed tokenised data by replacing the tokens with their original values.

Tokenisation can be applied to data that is not required to be processed by the service provider and is commonly used to protect sensitive information such as account numbers, phone numbers, email addresses, and other personal identifiable information.

Tokenisation does not reduce the security or compliance requirements, but it could reduce the complexity of their implementation.

Control Objectives:

- Minimise the amount of data that needs to be shared with a third party.
- Provide assurance that only authorized parties can gain access to the data.

Considerations for Controls

The security and robustness of a tokenisation system is dependent on many factors and the FI should ensure that following controls are considered in the implementation of tokenisation in a cloud outsourcing arrangement:

1. Careful risk assessment and evaluation should be performed on the tokenisation solution to

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

identify unique characteristics and all interactions and access to the sensitive data.

2. The CSP must not have any means to restore the tokens to the original data values such as access or control over the tokenisation system or tokenisation logic.
3. Systems that perform tokenisation be managed by the FI through access controls or other available CSP's security management tools to ensure security of the token pairs.

8. User Access Management and Authentication

User Access Management provides controlled access to information systems allowing staff, business partners and suppliers to perform their business activities, while protecting the information and systems from unauthorised access.

The full life cycle of user access management should be considered when implementing a cloud outsourcing arrangement. This includes the definition of identity and access management requirements, approval, provisioning, credential management, access review and revocation.

Control Objectives

- Ensure the confidentiality and integrity of FI's data.
- Authorize user access only to the information assets they require to perform their role.
- Ensure segregation of duties is in place for sensitive roles.
- Ensure least privilege principle is adhered to for user access management.

Considerations for Controls at CSP

1. For each cloud deployment there will be a management account (previously known as master account). This account should only be used for emergency, and not for day-to-day operations.
2. Identity and Access management should be of paramount consideration when performing a cloud outsourcing arrangement and should incorporate both technical and business user access management. A clear business owner should be identified for defined roles/access groups to ensure accountability, and ownership of each role defined.
3. An FI's Identity and Access management policies and standards should be applied in full in the CSP for Production and UAT environments used by the FI to ensure consistency.
4. Where federation of Active Directory credentials is used, or another cloud-based directory leveraged, the directory synchronization model, security requirements and redundancy controls for any synchronization tools should be reviewed and approved.
5. Multi-factor authentication and IP source restrictions should be strongly recommended for user access.
6. Where identity and access management assets reside in the cloud, strategies should be created and tested for migration or exit planning.
7. Scenarios which address recovery from a cloud directory compromise and synchronisation with on premise platforms should be added to disaster recovery and cyber security runbooks.
8. Integration with personnel system directory tools should be considered to ensure timely disabling of user's primary access, or to trigger a review of access rights for potentially toxic combinations.
9. User Access Administration should be subject to strict segregation of duties and maker / checker controls, especially where the CSP has access to or is managing systems or software. Changes in role access rights should be regularly reviewed by an independent assurance function or the role's owner.
10. Access and usage of service, generic and administrator accounts should be controlled via appropriate privileged user access management controls and activities logged for review.
11. Where development, QA and production environments exist in the cloud, access should be strictly controlled. Developers and Testers should not have any write access to production environments. Production support should have limited read access in accordance with their

responsibilities.

12. Where CSPs have access to the FI's systems or software, this should be captured in an identity and access management document, which should be reviewed at least annually for the accuracy of requirements, and that the configuration in the document matches the system state.
13. FI should document and maintain user access matrix, which defines access and privilege per role/user.
14. FI should record all entitlements to their workloads in central system. They should establish a regular review process for these entitlements and communicate any changes to the CSP.
15. FI should establish periodic review of user action logs as per defined log review use cases.

9. Privileged User Access Management

Whether infrastructure and applications are supported by the CSP of the FI, there should be a framework in place to define which system components are considered critical and what controls should be in place to manage privileged or administrative access to them.

The FI should ensure that privileged accounts are managed so that the CSP should only have access to its information assets by authorized exception.

Where IaaS, PaaS, or SaaS is used, the FI should consider the mode by which they are notified of material changes to the CSP's IT environment and can review the changes. CSPs can help FIs maintain appropriate oversight of material changes by establishing dedicated compliance programs that facilitate engagement between the FIs and the CSPs.

Control Objectives

- Ensure the confidentiality and integrity of FI's data.
- Manage privileged user access appropriately.
- Detect unauthorised or erroneous changes.

Considerations of controls at CSP

1. Users with privileged system access should be clearly defined and subject to regular user access reviews.
2. Privileged User access should be clearly tracked and reported and be linked to an agreed and approved change request when related to the FI's data. Note it is not always necessary for the CSP to disclose change requests to the FI.
3. The Privileged User Administration function should adhere to segregation of duties principle.
4. Privileged User Access should be in line with the "never alone" principles laid out in the MAS Technology Risk Management guidelines. There may be high risk situations where a break glass procedure is required, and dual controls circumvented. These situations should be defined in advance and subject to rigorous after the face reviews to provide assurance that no erroneous or unauthorized changes were introduced.
5. Access to critical information assets using privileged user access should be monitored.
6. Multifactor authentication should be mandated for privileged access to material workloads.
7. Cloud Security Posture Management ("CSPM") should be used to identify any security misconfiguration.
8. As the administrator account to the CSP cloud management console cannot be locked out, FI should monitor for unauthorized access to the accounts or password guessing attempts to break into the account. FIs should consider changing the password periodically.

10. Administrative Remote Access

Remote access is a tool often used by the FI or the CSP to allow connectivity from a remote location

to allow administration, system maintenance or software releases, as well as system support.

The inherent risk of allowing access from a remote location means that information and physical security controls of the Data Centre can be by-passed, so strict controls are required if it is to be permitted.

There are two aspects to cloud environments that need to be considered:

- Remote access to the systems by the CSP to manage its own systems.
- The various levels of remote access by the FI to both the platform and the systems that are in the cloud environment.

Control objectives

- Provide assurance that remote access to systems is secured against threats of impersonation.
- Provide assurance that user management controls are present and monitored for suspicious activity.
- Grant privileges in accordance with the requirement of the role, with appropriate segregation of duties.

Considerations of Controls

1. FIs should define and document all enabled remote access interfaces and assign critically to identify the risk profile.
2. Detailed documentation of all systems remote access procedures including security controls management. This documentation should be regularly reviewed to ensure accuracy and currency.
3. Remote access controls should be defined to ensure that there is a secured and auditable method of accessing systems and data.
4. Remote access security measures such as multi factor authentication or Virtual Private Network (“VPN”) encryption should be implemented.
5. End User Computing device controls should be considered, for instance access only from recognized hardware using machine authentication, or virtual desktops interfaces to reduce risk of malware contamination or unauthorized access.
6. Privileged remote access should only be permitted by authorized exception or break glass procedures and be time bound. Privileged remote access is inherently risky and must be strictly controlled.
7. All privileged remote access is to be reviewed on periodic basis for appropriateness by independent and qualified personnel.
8. All remote access channels should be encrypted and monitored.
9. Where possible, FIs should implement a direct private connection from their data center to the cloud environment and restrict all direct remote access to the cloud environment over the Internet.
10. The FI should consider restricting network access for remote access users. Jump boxes should also be considered for additional security.
11. All default accounts and access should be disabled.

11. Data Loss Prevention

The adoption of cloud services requires that an FI's data is transferred from the enterprise perimeter and control environment into the cloud. The cloud presents unique challenges where misconfiguration of the environment may result in data being exposed and accessible to the public. Controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.

In addition, the adoption of cloud services also makes it a challenge to detect and differentiate between the legitimate and unauthorized data exfiltration. Shadow IT use of unapproved cloud applications introduces compliance and security risk where the services do not adhere to compliance and security requirements. It is therefore essential that FIs monitor for both sanctioned and unsanctioned applications.

Considerations for the protection of data transmitted to and stored in the cloud must include all methods of ingress and egress. The FI should have in place a holistic data loss prevention strategy which includes data in transit, at rest and end point security controls.

Control Objectives

- Enforce the use of sanctioned cloud applications.
- Manage data processed and stored in the cloud environment in accordance with the FI's information security policy.
- Permit users access only to information assets based on least privilege principles.
- Prevent unauthorized or unintended dissemination of data.

Considerations of Controls

1. FI should document all mode of data transmission and data storage locations and ensure that DLP controls are uniformly applied for all these data access /storage interfaces. Controls should be commensurate with the nature of risks associated with the service arrangements.
2. The FI should consider having an agreement with the CSP to be informed of any data discovery related activities that involved the FI's data.
3. The FI should review their information asset classification framework to ensure that encompasses considerations for the cloud.
4. The FI may wish to consider enhanced controls for high value information assets that reside in the cloud such as strong encryption, tokenisation and logical segregation.
5. For hybrid cloud implementation where data in transit crosses on-premises or cloud deployments content inspection technologies should be deployed. Where possible, data loss prevention controls such as cloud access security broker should be implemented to monitor and control the access of the information.
6. For FI hosting sensitive information such as PII on cloud, FI should conduct periodic due diligence on the cloud outsourcing arrangement to ensure appropriate controls are in place.
7. The FI should perform periodic reviews of the users that are able to approve exceptions to DLP policies.
8. FIs should monitor the ingress and egress points for the use or adoption of unsanctioned cloud applications to support internal business processes or operations.
9. FIs should include a scenario for data loss in their incident response plan.
10. Data loss prevention controls should be implemented to secure access and extraction of PII information from the cloud services.
11. FIs should analyse changes in the use of the cloud services to detect suspicious and anomalous activities in cloud environment and unusual access to the data.
12. FI should have a Data Loss Governance and risk management framework defined which also deal with the risk of data loss arising from the cloud outsourcing arrangements. Templates and patterns for sensitive data should be defined, and metrics regularly reviewed.

12. Source Code Reviews

Above and beyond the typical secure SDLC the methodology for cloud applications, new methodologies such as DevOps requires explicit consideration of the integrity of code artefacts and of environments where applications are developed and tested throughout each development

iteration. The ability to compile, change and deploy the source code but also be able to secure the destruction of data and perform a clean breakdown of environments must also be considered.

Source code reviews are typically automated within formalized release management processes by the FI development teams (please see the section on DevOps for more detail).

Control Objectives:

- Ensure confidentiality and integrity of source codes, other code artefacts (e.g., compiled, and non-compiled codes, libraries, runtime modules)
- Prevent unauthorized alteration of code and system configurations.

Considerations of Controls

1. Guidelines for secure by design software development should be clearly defined and all developers trained on these approaches. Common considerations include coding approaches to ensure that OWASP Top 10 security risks do not occur, and that applications fail safe in the event of unexpected behaviour.
2. Content version controls, and strict processes for the migration of source code from one environment to another should be clearly defined as part of a release management process.
3. Segregation of duties can be accomplished in an automated fashion by introducing a CI/CD pipeline for static source code / application testing across the different environments, depending on the type of the cloud.
4. Access to source code repositories and privileged access to the development and testing environments are restricted to only specific authorized individuals. Escrow arrangement with vendor should be in place in case of source code access is required.
5. The processes supporting release management should ensure that source code is updated and compiled in a secured environment subjected to reviews (automated or manual) and cannot be tampered with by the author after it has been reviewed.
6. Automated source code applications should be regularly updated and reviewed to ensure currency and accuracy of their findings.
7. The source code should be regularly updated with new security patches and tested regularly for new vulnerabilities.

13. Penetration Testing

Testing the security of applications and infrastructure provides assurance of the security posture of a service. Using regular vulnerability assessments and periodic penetration tests, assurance can also be gained as to the effectiveness of security hardening and patching. Cloud environments provide a unique challenge as testing is performed on a shared platform. Test tools are not able to differentiate between flaws that can be exploited to cause damage and those that cannot. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.

Penetration Testing (PT) is necessary and applicable where cloud providers host external facing applications and process essential customer data. Some cloud environments have restrictions on the type and times of PT that can be conducted.

Please refer to the ABS guidelines of Penetration Testing and Red Team: Adversarial Attack Simulation Guidelines for further details.

Control Objectives

- Identify vulnerable configurations and provide assurance as to the security posture of a service.
- Provide assurance of security processes including security patching and hardening

Considerations of Controls

1. CSP penetration test reports can be used to gain assurance over the security of underlying systems, but the scope should be reviewed to fully understand what has been tested to ensure that the final testing encompasses all the systems involved in the provision of the service(s). PT should be performed by an independent party.
2. In addition to latest cyber threats, the tests should also take into consideration the threats that are unique to cloud computing, such as hypervisor jumping and weak application program interfaces.
3. Testers should be aware of typical security issues that are particular to cloud environments and virtualisation to understand the types of issue that may exist in such an environment.
4. FIs should engage the CSP prior to engaging PT to understand any technical limitations of testing and ensure awareness.
5. All vulnerabilities should be risk assessed, tracked, and managed / treated appropriately.
6. Where the vulnerability is on a system not managed by the FI, there needs to be an agreed upon remediation SLA that the CSP aligns to and disclose to the FIs.
7. In case responsibility for penetration tests on CSP side (i.e., in a SaaS model) proper governance over this program should be in place. The FI should ensure that all weaknesses and vulnerabilities are identified, risk assessment is conducted, and gaps closed with priority adequate for specific risk rating and in agreed timelines. Closing gaps conditions may be regulated with the service contract between CSP and FI. In case of gaps that cannot be mitigated an exception process should be triggered.
8. An FI should consider using a Red Teaming approach to testing the CSP's environment. It is also recommended that testing is performed on live systems subject to safety protocols to prevent any disruption of service.

14. Security Events Monitoring

The monitoring of the cloud environment for security events and incidents should be centralized to provide the FIs a single pane of glass for situational awareness and incident response. The activities in the cloud environment should be logged at granular levels which provide useful information for the investigation of security events and incidents. Such information should be consolidated and correlated centrally for security incident monitoring and detection. This would allow FIs' to leverage on existing incident response processes for the security incidents and events in the cloud.

Control Objectives

- Ensure log information are secured against unauthorized access and tampering.
- Verify that activities in the cloud are logged and correlated to detect security events and scenarios.
- Ensure security events and incidents in the cloud environment are detected and responded to in a timely manner.

Considerations of Controls

1. Consolidation of logs to a centralized system should be in place to ensure that the integrity and availability of the logs are maintained. The centralized log server should be secured and segregated from the operational environment to prevent unauthorized or accidental purging of the log information.
2. Logs should be streamed back to the FI for security incident and event correlation.

3. FIs should identify specific cloud security incident scenarios and develop specific correlation rules to detect such events. Where necessary, log parsers and correlation rules should be customized for such events and incident. The log parsers and correlation rules should be reviewed on regular basis to reduce false positive and improve alert quality.
4. Appropriate monitoring infrastructure such as a Security Incident and Event Monitoring (SIEM) system should be in place to provide automatic analysis, correlation, and triage of security logs from the various monitoring systems.
5. An approach to leverage the data from the CSP's SIEM architecture into the FI's core Intrusion Detection capability should be considered if possible.
6. FIs should consider the use of security analytics with machine learning capabilities to develop baseline to detect potential anomalies in the cloud environment. The scope of analysis should cover monitoring of the cloud capacity.

15. Securing Logs and Backups

Most systems can produce logs and may require backups. Whilst often overlooked, securing these logs and backups need careful consideration to ensure the confidentiality, integrity, and availability of this data. Both data in the direct control of FI and the CSP must be appropriately secured.

Control Objectives

- Log data should have robust controls to ensure their confidentiality and integrity.
- Log data should not contain sensitive information.
- Ensure the confidentiality and integrity of backup data.

Considerations of Controls

1. FI application development teams should ensure that no customer PII (Personal Identifiable Information) is logged.
2. The FI should establish requirements for forensic investigation including how to ensure that log data can be acquired in a streamlined sound manner.
3. The FI should have the appropriate access control in place for backups and log data.
4. FIs should consider the contents of backups and encrypt sensitive data where appropriate.
5. FIs should give due consideration to the management of encryption keys used for backup purposes.
6. The capability to recover data in a usable form should be regularly tested by the FI. Such restoration tests must be conducted securely to minimise any risk of data leakage.
7. Snapshots should be considered to enhance RPO capabilities particularly for critical databases or systems of record. These should be timed ahead of key activities such as cut off times or End of Day batch procedures.
8. Secure and robust security logging infrastructure should be leveraged.
9. Retention of the log should be aligned with FI record retention policy.

C) Run the Cloud

1. Change Management

It is expected that the FI maintains effective control over their data although it resides at the CSP. The CSP should have controls in place that facilitate management, near real time capability to review any privileged activities to ensure any changes are in line with approved processes.

FI should consider the mode by which they are notified of material changes to critical features or functions. CSPs can help FIs maintain appropriate oversight of material changes by establishing

dedicated compliance programs that facilitate engagement between the FIs and the CSPs, and support notification of such changes.

Control Objectives

- Ensure that all the changes follow a robust change management process that provides oversight commensurate with their risk. This includes changes managed by the CSP for IaaS, PaaS, and SaaS environments.
- Ensure heightened oversight of major changes that could impact the stability and/or security of the cloud operating environment.
- Detection of unauthorised or erroneous changes.

Considerations of Controls

1. Change management process should be mutually agreed between the CSP and the FI to ensure that expectations for emergency and standard changes are aligned. Such procedures should be formalised, and include change request, notification, and approval procedures.
2. Procedures for emergency and standard changes should be agreed, including the roles and responsibilities, and defined change windows for patching and software releases.
3. Where DevOps practices are being used, FIs should define conditions and scenarios that allow automated testing and releases. It is important to ensure that there is a full audit trail, record of the changes and evidence of pre-approval with segregation of duties in place.
4. FI should ensure that there is a process in place and scenarios defined where the CSP is required notify in advance of changes to critical services. Where appropriate, the FI should consider opportunities to test the deployment before those changes are implemented in their environment.
5. Change management governance should be incorporated into regular Service Level Management meetings.
6. FIs should review the change management procedures of the CSP, which should be independently assessed in line with OSPAR, SOC2 or other controls assessments.
7. FI should ensure that CSPs have well-defined change windows, testing and rollback plans, and an internal signoff procedure for any material changes that need to be implemented by the CSP. This can be evidenced via independent control testing.
8. FI should conduct post change testing where critical business functions may be impacted, including documented and evidenced test cases.
9. FI should consider conducting rollback and recovery testing to ensure that system changes can be reverted timely, in the event of failed deployments.

2. Configuration Management

Cloud is a dynamic environment where the core infrastructure can be set up and modified rapidly in response to business and operational needs. Hence the configuration management of the software defined environment is critical for the safe and secure operations of the cloud and information assets. FIs should implement monitoring to detect unauthorized changes to the cloud environment. Where possible, FIs should implement automated recovery to mitigate high risk changes.

Control Objectives

- Prevent unauthorized changes to the cloud environment, and ensure such changes are detected and remediated to prevent high impact incidents.

Considerations of Controls

1. Roles for the configuration of the cloud environment should be clearly defined, and segregation of duties should be considered for the design of the cloud roles for both the FIs and CSP.

2. At minimum, the infrastructure, security, and application roles should be segregated to prevent environmental changes which would allow the security controls to be bypassed.
3. Privilege for the infrastructure changes should be managed centrally, and the configuration of the environment should be closely monitored for unauthorized changes.
4. FIs should consider establishing standard server images or implementing Infrastructure as Code ("IaC") for consistent and secure creation of new servers. Changes to IaC should be managed under DevSecOps process as part of CI/CD pipeline.
5. Key environment changes should be monitored and automated alerts should be triggered to alert the security or the infrastructure team.
6. FIs should create baselines configurations, establish a process to review the baselines periodically, and monitor deviations from the baselines.
7. Where possible, for high impact changes to critical business services, FIs should implement auto-remediation to revert the environment to the baseline configurations.

3. Event Management

The monitoring of infrastructure events is a responsibility that both the FIs and the CSP share. The FIs are responsible for monitoring events that can impact the stability and or availability of their applications and systems. Based on the service model, the CSP is usually responsible for events that impact the underlying infrastructure of the FI's workloads, which could include the virtual environment, containers, or customer workloads.

Control Objectives:

- Define and monitor key events to ensure the confidentiality, availability and integrity of the cloud environment is not compromised.
- Provide early detection of network and system anomalies in the IT environment to facilitate timely response to potentially developing technology and security incidents.
- Manage and escalate events appropriately according to their criticality and assigned ownership.

Considerations for Controls

1. FIs should ensure there is a framework to determine the event categorization, based on impact to the FI, responsible parties and actions required with corresponding timeline, clearly defined. Appropriate detection mechanisms should be in place at the network, system, and application level to analyse events that could affect the security and stability of the cloud service.
2. Security and technology events and the various levels of severity should be appropriately defined, and ownership agreed between the FI and the CSP.
3. FIs should consider the use of automated ticketing upon the detection of incident to improve turnaround for the response team.
4. FIs should consider sending key event logs from cloud workloads to the FIs' SIEM to ensure timely alert and monitoring.
5. SLAs for critical events should be established between the FI and the CSP. This should be done in accordance with an escalation matrix to notify the appropriate parties.
6. Events that have been rated as material should be immediately visible in network or technology operations centres so that they can be responded to in a timely manner.
7. The FI should define playbooks for recovery scenarios along with key roles and task ownership.

4. Incident and Problem Management

Timely detection of critical incidents coupled with tight integration with incident response and management processes can allow incidents to be remediated speedily, thereby limiting downtime or potential data breaches.

Cyber-attacks, the compromise of a computer system, and unplanned outages can only be detected in a timely fashion if there is effective monitoring of the IT systems to differentiate legitimate and abnormal activities. As attack sophistication increases with the complexities of modern IT systems, it is imperative that monitoring of IT systems progresses beyond typical health and performance metrics to include security events and advanced analytics to correlate events across various systems at the network, infrastructure, and application layers of the IT environment.

Control Objectives:

- Provide a reasonable level of retrospective detection of security incidents in the IT environment as and when new threat intelligence is available.
- Provide assurance that technology and security incidents are appropriately escalated and notified to the relevant stakeholders for management action.
- Provide assurance the incidents in the environment are properly reviewed and identified gaps are remediated to prevent a reoccurrence.
- Ability to adhere to the relevant regulatory requirements (e.g., M A S Notices on Technology Risk Management)

Considerations of Controls

1. Criteria and performance requirements i.e., SLA for the escalation, notification, containment, and closure of relevant security and technology incidents should be appropriately defined and agreed between the FI and the CSP, especially where regulatory instruments such as Directives and Notices stipulate timelines.
2. Learning points captured from past incidents as knowledge articles for continuous improvement to the process.
3. Access to appropriate reports on relevant incidents and root cause analysis should be agreed between the FI and the CSP. Where the CSP has commercial, security or intellectual property reasons to not disclose such reports directly to the FI, the use of a mutually acceptable independent 3rd party can be agreed.
4. CSP should provide reasonable access to necessary information to assist in any FI investigation arising due to an incident in the cloud, to the extent that it is does not contravene any other legal obligations.
5. Incidents that have considered to have a material impact to the FI should be subject to formalized post incident reviews and problem management.
6. Where common occurring incidents become formally recognized as systemic issues, Problem Management should be put in place to ensure that an appropriate remediation is identified and implemented.
7. Metrics on incidents and problem tickets should be regularly reviewed and discussed at the cloud governance forum.
8. A Computer Emergency Response Team (CERT) or Security Incident Response Team (SIRT) should be in place to provide timely response to security incidents. Coordination between the CSP and FIs' teams should be formalised.
9. Appropriate security systems and measures, such as network intrusion detection/prevention systems (NIDS/NIPS), web application firewall (WAF), DDoS mitigation, and data leakage prevention systems, should be deployed at strategic locations to detect and mitigate security breaches and ongoing attacks.
10. Based on the materiality of the outsourcing arrangement, integration into a Security Operations Centre (SOC) and / or Technology Operations Centre (TOC) operating on a 24x7 basis should be strongly recommended to provide active monitoring of security events,

technology incidents and ensure timely escalation and management of issues.

11. While it is recognized that it is usually the FI's responsibility to identify a relevant incident under relevant MAS Notices related to Technology Risk Management, there are situations where systems or applications designated MAS Critical may be fully managed by the CSP, particularly SaaS or white-labelling. In these situations, a contractual requirement should be included to ensure notification to the FI as soon as possible after the detection of a relevant incident. The FI is then required to notify the MAS within 60 minutes of receiving the notification. The CSP should include as much information as possible in this notification to allow for the required regulatory submission. If all data points are not available at that time the CSP should ensure these are delivered within a reasonable timeframe, which should not exceed 24 hours after the original notification.
12. Review and testing of the incident response plan should be conducted on a regular basis by the CSP and involve the FI where appropriate.

5. Capacity Management

The FI should have a clear view of its requirements to operate its resources to ensure that business functions can proceed without any interruptions. The FI and CSP both have clear lines of responsibilities, but it is imperative that the FI have insight into their workloads running on the cloud and an SLA defined.

Business functions may have period spikes or strategic growth ambitions which technology should be aware of.

Control Objectives

- Business volumes are well understood, and that capacity exists to support them.
- Resources are monitored appropriately to understand average utilisation and peaks.
- Systems have appropriate resources to allow for resiliency in the event of failure or unplanned outage.

Considerations of Controls

1. FIs should review and approve the cloud architecture to have sufficient capacity for the service outsourced at the design stage.
2. The FI's technology operations team should monitor and review capacity utilisation and review where capacity may be at risk. Planning for upgrades, enhancements including funding requests should be regularly discussed in internal governance forums.
3. The FIs need to ensure that business strategies and requirements, including special events such as index rebalancing, special business marketing campaigns expecting high user traffic, are taken into consideration when reviewing the capacity of their workloads.
4. Automated increase of capacity should be considered and such thresholds to be regularly reviewed.
5. Performance testing (e.g., load test or stress test) should be considered periodically and on ad-hoc basis upon major system changes or pre-special events to simulate workloads anticipated for cloud resources re-allocation or scale-up.

6. Patching and Vulnerability Management

The security of the systems and infrastructure of the cloud environment is a shared responsibility especially for platform and infrastructure as a service engagement. Given the ease of software purchase and implementation in the cloud environment, FIs need to detect and remediate the vulnerabilities in the cloud environment swiftly.

Control Objectives

- Ensure there is clear ownership of all assets in the cloud environment, and that their criticality is rated.
- Swiftly identify potential vulnerabilities and system instabilities.
- Swiftly and safely deploy security and operating system patches.

Considerations of Controls

1. FIs should maintain an inventory of the software used in the cloud environment.
2. FIs should have documented contract with CSP for assigning responsibilities to assess, track and remediate the vulnerabilities periodically announced by the respective technology software and hardware vendors.
3. The software inventory should also be used to track software life cycle so that informed decisions can be made to replace or have mitigating controls.
4. FIs/CSPs should remediate the vulnerabilities in accordance with their criticality.
5. Where possible, FIs should containerized their applications in the cloud environment to facilitate prompt patching while minimizing impact to the cloud workload.
6. The FI should work with the CSP and understand capabilities in their offerings that would help best with vulnerability and patching management.
7. The CSP should be able to demonstrate the status of their compliance with published vulnerabilities and their ability to patch when required.
8. In events where the patches cannot be applied to address the vulnerabilities promptly, FIs should consider the use of security controls (e.g., network access control, intrusion prevention systems) to mitigate the risk of exploit.
9. An exception process needs to be created for any vulnerabilities that cannot be remediated.
10. FIs contract with CSP should cover frequency of vulnerability scanning and patching cycles. For critical assets, stringent scanning cycle may be designed.
11. For SaaS, CSP should be solely responsible for vulnerability identification and remediation.
12. For IaaS, FIs should follow their respective organization's vulnerability and patch management policy and procedures.
13. For PaaS, FIs and CSP to follow agreed roles and responsibility in the contract for vulnerability and patch management.
14. Emergency patching process should be created for priority vulnerabilities identified that need immediate remediation.

7. Collaborative Disaster Recovery Testing

Disaster recovery testing is an essential part of developing an effective disaster recovery strategy. Where there is business critical function, the FI should plan and perform their own simulated disaster recovery testing, testing jointly with the CSP where possible. If relevant, the outsourcing arrangement should contain Business Continuity Planning (BCP) requirements on the CSP, in particular, Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Control Objectives:

- Ensure the continued availability of services commensurate with their criticality in the cloud environment.
- Ensure that data, systems, and applications can be recovered within the timeframe required by the FI.

Considerations of Controls

1. The CSP should develop disaster recovery and business continuity plans and where appropriate share the plans with the FI.
2. The FIs should ensure that CSPs have snapshots of critical databases or systems of record for disaster recovery / business continuity.

3. Ensure that all changes in the computing environment are reflected in the disaster recovery plan, and that all facilities are available.
4. There should be a communications plan or an automated call tree that covers both CSP and FI staff.
5. FI should be aware of the CSP's recovery plan based on the contractually agreed service (SaaS, PaaS, IaaS) provided by the CSP. Integrate the CSP key point of contacts and processes, as applicable, into the FI incident and crisis management process.
6. The FI should develop disaster recovery plans for its assets in the cloud, and test these at least annually. Tests should be validated for accuracy, completeness, and validity of recovery procedures.
7. FI and CSP personnel involved in disaster recovery procedures should be aware of their responsibilities and capable of executing them. These should be tested at least annually.
8. CSPs should obtain necessary certifications for disaster recovery (e.g., ISO27001 and ISO 22301) and their processes should be audited by independent third parties with such audit reports made available to the FI.
9. When performing DR testing with the CSP, FI to consider doing testing on short notice to validate their level of readiness for an actual disaster event.
10. FI to ensure that any deficiencies noted during testing are recorded, and the implementation of corrective actions is monitored via the appropriate governance bodies.
11. Various disaster recovery cloud resilience scenarios including both component failure, full site loss and partial failures should be incorporated into the FI testing plan. These scenarios should be tested according to a strategy defined by the bank in line with its business continuity policy.
12. The scalable and redundant nature of cloud outsourcing arrangements allows for more rigorous testing, including the failure of active-active configurations. It is recommended to regularly test these capabilities, and to keep services failed over for an extended period to validate operational stability.

Acknowledgements

The ABS SCCS Cloud Computing Implementation Guide Working Group Members:

1. ANZ Bank
2. Barclays Bank
3. Bank of America
4. BNP Paribas
5. Citibank
6. Credit Suisse
7. HSBC
8. JP Morgan
9. OCBC
10. UOB

APPENDIX

A. Service Models

Infrastructure as a Service (IaaS). The capability provided to the organisation is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service (PaaS). The capability provided to the organisation is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service (SaaS). The capability provided to the organisation is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

B. Deployment Models

Private cloud. The cloud infrastructure is provisioned for the exclusive use by a single organization comprising multiple consumers (e.g., business units). 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.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and 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.

Public cloud. The 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 provider.

Hybrid cloud. The 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).