ABS Cloud Computing Implementation Guide 2.0

for the Financial Industry in Singapore

The Association of Banks in Singapore

Table of Contents

Section 1: Introduction

Objective

The Association of Banks in Singapore (ABS) has developed the second version of the implementation guide for Financial Institutions (FIs) to use when entering into Cloud outsourcing arrangements, as well as the on-going management thereof.

Technology and market practice has advanced rapidly since the guide was first released in June 2016. It was felt an updated version was required to address these changes, as well as to further support the practice of migrating material workloads to the Cloud, including systems of record and those classified as Monetary Authority of Singapore (MAS) Critical[1].

The recommendations that lie within have been discussed and agreed by members of the ABS Standing Committee for Cyber Security (SCCS) with the intent to assist FIs in understanding approaches to due diligence, vendor management and key controls that should be implemented on an on-going basis in Cloud outsourcing arrangements.

Additionally it can be used by Cloud Service Providers (CSPs) to better understand what is required to achieve successful Cloud outsourcing arrangements with FIs.

The guiding principle 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 should apply.

It should be noted that this document contains best practice recommendations and considerations and is intended to support the safe adoption of Cloud. It is not a set of mandatory requirements.

The adoption of Cloud can offer a number of advantages, including faster time to market, scalability, cost savings, enhanced security and access controls. This guide includes recommendations for due diligence and controls that address the typical characteristics of cloud services, such as multi-tenancy, data commingling and higher propensity for processing to be carried out in multiple locations.

These guidelines are set out in the three following sections:

- Section 2 addresses Cloud outsourcing classifications and how these should influence decision making in Cloud outsourcing agreements.
- Section 3 addresses a minimum set of activities recommended as part of due diligence before entering into a Cloud outsourcing agreement.
- Section 4 addresses the minimum set of controls recommended when entering into a Cloud outsourcing arrangement as well as the enhanced set of controls recommended for Material outsourcing, including critical workloads.

Definitions

This definition of Cloud is taken from the National Institute of Standards and Technology (NIST).

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.

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

[1] Please refer to MAS Notice 644 for the definition of MAS Critical

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.

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.

On premises private Cloud may also be considered in a similar manner to this, where a CSP deploys infrastructure at the premises of the organization for its exclusive use. The organization can also assume responsibility for the environmental and physical security controls as a result. For On Prem services the FI should reference the MAS Technology Risk Management Guidelines, but may want to reference controls in this Guideline where appropriate.

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).

Outsourcing

An "outsourcing arrangement" means an arrangement in which a service provider provides the institution with a service that may currently or potentially be performed by the institution itself and which includes the following characteristics–

(a) the institution is dependent on the service on an ongoing basis; and

(b) the service is integral to the provision of a financial service by the institution or the service is provided to the market by the service provider in the name of the institution

Please refer to the latest version of the MAS Outsourcing Guidelines and FAQ for further clarifications.

Section 2: Cloud outsourcing classification

In this section, guidance is given as to the definition of differing risk categories in Cloud outsourcing arrangements.

Guidance is also given as to what is likely to constitute material and non-material outsourcing in the context of cloud.

This allows an FI to assess the inherent risk profile of a Cloud Outsourcing arrangement, and then ensure that appropriate controls are in place to ensure that residual risks are appropriately managed and monitored and thus remain within appetite.

For clarity as to the definition of materiality, an extract from the Monetary Authority of Singapore (MAS) outsourcing guidelines is included:

“material outsourcing arrangement” means an outsourcing arrangement

(a) which, in the event of a service failure or security breach, has the potential to either materially impact an institution’s

(i) business operations, reputation or profitability; or

(ii) ability to manage risk and comply with applicable laws and regulations,

or

(b) which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on an institution’s customers.

For further guidance on material outsourcing arrangements please to the prevailing version of the MAS Outsourcing Guidelines[2].

The materiality of an outsourcing arrangement should dictate the types of controls deployed, as well as the depth and breadth of any initial, and on-going, due diligence.

The below table is for guidance only, please refer to the MAS Outsourcing guidelines for further examples of material outsourcing. Any decision should be made based on the FI's risk appetite and formalized at an appropriate governance forum. It should also be noted that not all use of Cloud may constitute outsourcing: services such as content delivery networks, survey portals may be considered a subscription service, and thus not subject to the same level of oversight as a Cloud outsourcing arrangement.

Cloud Outsourcing Category	**Common characteristics**	**Examples**
Non Material	• Staff data which does not include bank account or credit card data (e.g. information on name cards) • Development and Test environments • Services not defined as 'critical'	• Application binaries, or risk management quant libraries that are being tested on masked data (i.e. performance & volume testing, regression testing, or Monte Carlo simulations) • Information Security solutions such as Managed Security Services / Operations Centres,

[2] As of the time of publication refer to Annex 2 of the 2016 Outsourcing Guidelines

		where information assets are encrypted and logically segregated • Websites for accessing information that is classified as 'public' • Service Management applications
Material	• Use of customer information, the unauthorized access or disclosure, loss or theft of which may have a material impact on the customer • Use of staff data, including Personally Identifiable Information (PII), payroll and bank account or credit card data • Software used for the trading of financial instruments or other transactions • Financial Risk management systems (Market, Credit and Liquidity) • Non-public commercially sensitive information that could influence financial markets • Regulatory reporting or accounting data • Outsourced business activity as defined as critical by the FI • Systems of record, including core banking applications • Any Cloud based implementation of a system classified as 'MAS Critical'	• Email and document storage • Authentication services providing One Time Passwords (OTP) or 2 Factor Authentication (2FA) • Vulnerability Scanning Services

Once the classification of a Cloud Outsourcing arrangements has been defined, the below tables maps the category to the recommended minimum control environment as laid out in Chapter 4.

Cloud Outsourcing Category	**Recommended Controls**
Non Material	Considerations for Standard Workload
Material	Considerations for Material Workloads

Section 3: Activities recommended as part of due diligence

This section covers the recommended due diligence and vendor management activities for Cloud outsourcing arrangements. The recommendations will cover pre-engagement of the CSP as well as on-going risk assessment and oversight. Financial institutions should use a risk-based approach as well as an applicability assessment to determine the relevance of the recommended activities for their specific outsourcing arrangement.

1. Governance

The structure and manner that an on-going outsourcing arrangement is managed is paramount to maximising the benefits derived from it, and minimising and managing the inherent risks associated with outsourcing.

Cloud Computing Due Diligence Framework FIs should establish a risk management framework and conduct appropriate due diligence to manage the risks associated with CSPs as well as their material sub-contracting arrangements. It is recommended that an FI develop a framework to assist in the identification and monitoring of risks during cloud adoption.

Contractual Agreement. Expectations should be agreed between the CSP and the FI, in particular with regard to operational contract management, SLA management, technology risk management, business continuity management and contract exit. These are covered in details in other sections; however CSPs should provide assurance to FIs that there is stringent governance on their daily operational procedures, and is validated via independent assurance process.

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.

It is recognized that moving technology infrastructure into the cloud creates a shared responsibility model between the consumer and the CSP for the operation and management of security controls. Keeping in mind that the FI will remain accountable for protecting its information, it is strongly recommended to ensure that roles and responsibilities for relevant IT and operations departments are clearly understood, defined and contractually agreed before transferring any data into the cloud.

FI should perform due diligence to understand the services they are adopting and what their and the CSPs responsibilities are. Below is an example showing areas of consideration when defining responsibilities between an FI and CSP before entering into the outsourcing arrangement:

	IaaS	PaaS	SaaS
Content	FI Managed	FI Managed	FI Managed
Identity & Access Management	FI Managed	FI Managed	FI Managed
Application Security	FI Managed	FI Managed	CSP Managed
Deployment	FI Managed	FI Managed	CSP Managed
Privileged User Management	FI Managed	FI Managed	CSP Managed
Patching	FI Managed	To be Defined / Agreed	CSP Managed
Penetration Testing	FI Managed	To be Defined / Agreed	CSP Managed
Disaster Recovery Testing	FI Managed	To be Defined / Agreed	CSP Managed
Network Security	FI Managed	To be Defined / Agreed	CSP Managed
SIEM & Audit Logging	FI Managed	To be Defined / Agreed	CSP Managed
OS Management	To be Defined / Agreed	CSP Managed	CSP Managed
Storage	CSP Managed	CSP Managed	CSP Managed
Hardware	CSP Managed	CSP Managed	CSP Managed

Key Performance Indicators / Key Risk Indicators. Once responsibilities are understood and agreed KPIs, key activities, inputs and outputs should be defined in an SLA, along with accountabilities. The governance of the SLA as well as the tools recommended for the tracking should also be defined in the contract. KRIs should indicate the effectiveness of key information security controls, which are subject to periodic review. The control testing interval should be determined by the FI based on a risk-based approach. The FI's service level requirements and the metrics by which the relevant service is to be measured should also be documented clearly.

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.

Asset Classification. The FI should have a clear policy on the classification of the assets that are outsourced to CSP as part of its risk profiling. 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.

2. Assessment of the Cloud Service Provider

The due diligence on the cloud service provider must take into consideration data confidentiality, financial, operational and reputational factors including the level of ethical and professional standards held by the CSP and the CSP's ability to comply with its obligation under the outsourcing arrangement.

Materiality Assessment. Prior to engagement with a CSP, FIs need to establish the CSP's ability to comply with necessary minimum controls based on the intended workloads (see section 2 Cloud Outsourcing Classification).

Financials. The financial strength and resources should be assessed to ensure that the viability of the service provider to service commitments even under adverse conditions.

Corporate Governance and Entity Controls. The good corporate practices and control consciousness of CSP's staff sets the priority and culture, and is the foundation for all the other components of internal control, providing discipline and structure.

Data Centre. It is important for FI to be in position to ascertain and agree on which countries are acceptable for an FIs' data to be processed and reside. This determines the nature of the risk that exists in the outsourcing arrangement, and is a basic requirement to demonstrate that the FI has sufficient oversight of its outsourcing arrangement.

Physical Security Risk Assessment. A Threat & Vulnerability Risk Assessment (TVRA) or equivalent independent assessments should be conducted on data centres in Singapore and overseas where these data centres support the FI's Singapore operations. The purpose of this assessment is to identify security threats to and operational weaknesses in a data centre in order to determine the level and type of protection that should be established to safeguard it.

The scope of assessment is dependent on many factors such as the criticality and the type of systems hosted at the DC. Nevertheless, the scope should minimally include the DC's perimeter, physical and environmental security, natural disasters, and the political and economic climate of the country in which the DC resides. This assessment is commonly undertaken by the CSP. FI should obtain and validate the TVRA or equivalent independent reports from the CSP. The assessment must be performed periodically to identify any security and operational weaknesses. The CSP should promptly remedy any threats, risks or security issues identified as being material in the assessment report.

The assessment criterions are available at latest MAS Technology Risk Management Guidelines under data centres protection and controls.

Due Diligence Process. Due diligence of the CSP should cover all locations that support the FI's processing and data storage requirements. It should not be assumed that controls are consistent across all locations. If the CSP confirms that controls are consistent across all relevant locations, then a single assessment report for such locations should suffice.

The Association of Banks in Singapore (ABS) has established guidelines on Control Objectives and Procedures for the FIs' Outsourced Service Providers (OSPs) operating in Singapore, also known as OSPAR. These guidelines form the minimum/baseline controls that OSPs (which may include CSPs where relevant) which wish to service the FIs should have in place.

It is the FI's responsibility to assess the appropriateness of the scope and controls covered by the report. Domains such as information security policies and awareness, due diligence and risk assessment of practices related to sub-contracting, system vulnerability assessments and penetration testing, and technology refresh management of end of life systems are particularly relevant.

The FI must also ensure that the controls covered by the report provide the necessary assurance to support compliance with the MAS Technology Risk Management Guidelines (TRMG) and Outsourcing Guidelines.

It is strongly recommended to review the scope of such reports to ensure that the sample set selected by the independent auditor provides assurance of the services, facilities and locations that the FI intends to utilise.

Subcontracting. The MAS expects FIs retain the ability to maintain similar control over the risks from its outsourcing arrangements when a CSP uses a sub-contractor to support material services. As such, FIs should establish risk management frameworks and conduct appropriate due diligence to manage the risks associated with sub-contracting arrangements. FIs should retain the ability to monitor and control its outsourcing agreements when a service provider uses a sub-contractor to support material services. An appropriate notification method should be agreed between the FI and the CSP for changes in material subcontracting so that the FI can exercise oversight.

Pre and Post Implementation Reviews. FIs should establish their own outsourcing risk management framework and the necessary policies and procedures with respect to the scope of their pre and post-implementation reviews. These should commensurate with the materiality of the outsourcing arrangement.
Pre-implementation reviews should not be limited to the due-diligence on the CSP but also 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 institutions' controls in monitoring the performance of the service provider and checks to ensure that the risks associated with the outsourcing activity are managed appropriately as planned. Post-implementation reviews are usually conducted shortly after the commencement of the outsourcing arrangement. MAS expect institutions to determine an appropriate timeframe for these post-implementation reviews.

3. Contractual Considerations

MAS consider cloud services operated by CSPs as a form of outsourcing. When negotiating a contract with a CSP, the FI should ensure that it has the ability to contractually enforce agreed and measurable information security and operational requirements. Without such authority, any controls that are put in place as part of the outsourcing arrangement may not be enforced, as the FI will be relying on good faith efforts of the CSP.

Data Confidentiality and Control ownership. The FI should ensure that the outsourcing agreement includes the following requirements:

(a) State the responsibilities of contracting parties in the outsourcing agreement to address the scope of the services and the applicable baseline security policies and practices, including the

circumstances under which each party has the right to change security requirements. The outsourcing agreement should also address:

(i) the issue of the party liable for losses in the event of a breach of security or confidentiality and the CSP's obligation to inform FI; and

(ii) the issue of access to and disclosure of FIs' information assets by the CSP. FIs' information should only be used by the CSP and its staff strictly for the purpose of the contracted service, and in accordance with the terms of pertaining to such use

(b) Disclose the FI's information to the CSP only on a need-to-know basis;

(c) Ensure the CSP is able to 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; and

(d) Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, security adequacy and compliance in respect of the operations of the CSP, and requiring the CSP to promptly disclose to the FI any breaches or serious incidents that may impact FI's data confidentiality. CSP should have a defined framework for assessment of incidents (e.g. near-miss events resulting from repeated unsuccessful attempts or application errors resulting in data breaches) so that FI can take the necessary precautions to safeguard their data.

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

In the event of contract termination with the CSP, either on expiry or prematurely, the FI should have the contractual right to promptly render data inaccessible at the CSP's systems (including backups).

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 Transfers and Location of Data. The FI should consider the social, political and economic climate of a country before an FI agrees to have its data placed there. FIs should at the outset obtain legal advice to ascertain that the service cloud provider is operating in jurisdictions that generally uphold confidentiality clauses and agreement. An FI should enter into outsourcing arrangements only with service providers 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 come to an agreement where the FI's data can reside in respect of 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 outsourcing 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 in the event the local legal requirements compel the CSP to disclose the data to a 3rd party, bearing in mind the section 47 of the Singapore Banking Act.

An FI should not enter into outsourcing arrangements with service providers in jurisdictions where prompt access to information by MAS or agents appointed by MAS to act on its behalf, at the service provider, may be impeded by legal or administrative restrictions.

Refer to MAS outsourcing guidelines for details[3]*.*

Audit and Inspection. An outsourcing arrangement should not interfere with the ability of FIs to effectively manage its business activities, risk or impede MAS in carrying out its supervisory functions and objectives.

If an audit inspection cannot be performed by FI's appointed auditors, FIs may rely on the audit opinion of a service provider's external auditor. The party performing the audit should possess the requisite knowledge and skills to perform the engagement, and be independent of the units or functions involved in the outsourcing arrangement.

A right to audit by the MAS should be included as a stipulation in the contract.

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

Consideration should also be given to the support provided by a CSP during an audit, including resources, costs, and turn-around times for requests for information. Typically this will be a value add service by the CSP.

Business Continuity Management. FI should take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated such that FI remains able to conduct its business with integrity and competence in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the CSP. These should include taking the following steps:

(a) Determine that the CSP has in place satisfactory business continuity plans ("BCP"). Prior to contracting with the CSP, the FI should verify the CSP's ability to recover the outsourced systems and/or IT services within the stipulated RTO.
(b) Proactively seek assurance on the state of BCP preparedness of the CSP, or participate in joint testing in specific nature of outsourced services (such as SaaS or PaaS), where possible. FIs should ensure the CSP and FI regularly test its BCP plans and that the tests validate the feasibility of the RTO, RPO and resumption operating capacities.
(c) Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the FI will be able to continue business operations and that all documents, records of transactions and information previously given to the CSP should be promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable.

Refer to MAS' Business Continuity Management Guidelines for details.

Subcontractors. Where a CSP elects to use subcontractors to perform the services which have a material impact to the provision of the Cloud service, an appropriate notification method should be agreed between the FI and the CSP for changes in material subcontracting so that the FI can 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 outsourcing 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

[3] At the time of publication section *5.10 Outsourcing outside Singapore and MAS Notice 634 Banking secrecy – Condition for outsourcing*

managing their subcontractors and remediating any non-performance issues identified. Where the FI does not have the contractual right to reject any proposed subcontractor, it is recommended that the FI should retain a right to terminate the outsourcing agreement in the event of an unsatisfactory performance of the subcontractors, or the subcontractor is or has become prohibited by the regulator.

Service Level Agreements. Enforceable and measurable Service Level Agreements (SLAs) should be negotiated where possible, particularly for material outsourcing arrangements. These should include a definition of the governance 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 compound 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 included.

Data Retention. FI must be able to stipulate access to its data, both those used for daily operational purposes as well as 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 that its data is protected by verified and appropriate technical means through assessment as part of the due diligence process.

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

Upon exiting a contract with a CSP where FI does not have direct access to its data, FI needs to 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. In this way, CSP can provide assurance to the FI that its data is rendered permanently inaccessible in a timely manner, in particular any backup or distributed online media after the exit of the contract.

Default Termination. The contract should clearly stipulate the situations in which FIs should have the right to terminate the outsourcing agreement in the event of default, or under circumstances where:

- the CSP undergoes a change in ownership;
- the CSP becomes insolvent or goes into liquidation
- the CSP goes into receivership or judicial management whether in Singapore or elsewhere;
- there has been a breach of security or confidentiality; or
- there is a demonstrable deterioration in the ability of the service provider to perform the contracted service.

The minimum period to execute a termination provision should be specified in the outsourcing agreement. The outsourcing agreement should also contain provisions to ensure smooth transition when the agreement is terminated or amended.

Refer to the MAS outsourcing guidelines for details pertaining to default termination and early exit.

Exit Plan. The extent of exit planning should be dependent on the materiality of the outsourcing arrangement and potential impact to the on-going operations of the FI. The following considerations should be taken into account:

1. Agreed procedure and tools used for deletion of data in a manner that data is rendered irrecoverable.
2. Costs associated with the exfiltration of an FI's data.

3. Removal of all financial institution'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 the purpose of continuity of service.

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

5. 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 manner in which data is to be returned to the FI, as well as support from the CSP to ensure the accessibility of the data.
6. Data elements to be extracted and returned to the FI should be agreed upon at the start of the outsourcing arrangement and reviewed whenever there are material changes to the outsourcing arrangement.

Section 4: Key controls recommended when entering into a cloud outsourcing arrangement

This section of the implementation guideline details the recommended baseline controls that should be implemented for standard non material workloads, as well as additional considerations for material and critical workloads. Considerations for standard workloads are also applicable to material workloads

The Journey to the Cloud

A. Govern the Cloud (setup and on-going management)

- Organizational 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 which are planning to scale their outsourcing arrangements may need to consider adapting their organizational structure to ensure effective and timely oversight of 3rd parties, particularly with regard to performance, operational effectiveness of controls and remediation.

Control Objectives

- Execute robust and timely oversight of risks associated with cloud outsourcing arrangements
- Ensure there is accountability and governance in place that bridges the FI and CSPs
- Ensure that the FI has the appropriate skills and knowledge to execute oversight and manage demand
- Have a consistent, empowered interface between FI's business and operations divisions and the CSP

Considerations for Standard Workloads

1. Based on the model of shared responsibility defined during the contractual negotiations, an FI should design and implement a suitable governance body and roles, where appropriate with representatives of both the CSP and the FI. The governance body should be empowered to oversee adherence to SLAs, review KPIs and KRIs, incidents, security incidents and other relevant matters to the risks associated with outsourcing. This governance body should meet periodically, the frequency determined by the materiality of the arrangement.
2. It is recommended that metrics provide a complete view, both where controls are owned and operated by the FI or the CSP. Interfaces to internal governance bodies should also be considered for FI owned controls.
3. Execution of oversight of cloud outsourcing arrangements requires a specific skill-set. FIs should be mindful that when outsourcing that key staff and roles are identified and that their knowledge is kept up to date by training or other methods.
4. FIs should consider creating a specific role to execute oversight of cloud outsourcing arrangements.
5. 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.
6. Any incremental changes to outsourcing controls should be managed via the governance forum.

Considerations for Material Workloads

1. Where critical services have been outsourced representation on the governance body should be of appropriately senior technology and business representatives.
2. A single point of contact from the CSP should be formally identified and given a sufficient mandate.
3. A defined escalation procedure should be put in place for both the CSP and the FI to use.

2. Control Assessment & Monitoring

The FI should establish an appropriate control framework to manage the risks associated with the intended workloads. The controls should be defined in line with corporate policies and regulatory expectations and support compliance with these requirements. Where possible control testing should be automated and tested at a frequency determined by the FI's risk appetite.

Risk Assessment should be considered from two angles: firstly to assess the CSP, and secondly to assess a particular service or pattern 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 provide assurance of the effectiveness of the overall control framework
- Where non-compliance is detected trigger an appropriate and timely response for remediation

Considerations for Standard Workloads

1. Prior to embarking on any cloud outsourcing arrangement a thorough technical risk assessment of key controls should be performed based on the use cases.
2. Where possible an FI should ensure that a control failure triggers an automated response and notification.
3. The FI should consider leveraging the controls available in the cloud environment to enforce consistent security standards and baselines as well as automated remediation where possible.

Considerations for Material Workloads

1. FIs should assess their existing controls assurance framework for the suitability of managing cloud outsourcing. Key procedural controls must be identified, mapped and effectiveness thresholds defined.
2. Establish Management Information and dashboard material for reporting on control assessments. Define an appropriate oversight and escalation model to execute remediation activities which takes into consideration both FI and CSP owned activities.
3. FI should consider the use of analytics with machine learning (ML) and other best in breed technologies to develop baselines for compliance checks to highlight and avoid non-compliance.

3. Billing Models

Strategic adoption of cloud is usually supported by a business case. Additionally with a distributed model of consumption it is important to 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 in a timely manner
- Facilitate transparency in overall cloud usage for management information and strategic decision making

Considerations for Standard Workloads

1. It is recommended that the FI have a centralised governance structure to manage master subscription and control how that is provisioned for specific workloads.
2. Ensure that all assets in the cloud are identified, have clear ownership assigned and are rated for their asset classification.
3. Do not use the CSP's master account to centrally manage the costs, create sub accounts which are aligned to the finance structure of the FI.
4. Ensure there is training and educational material for users of the cloud environment which is tailored to help them understand the best adoption methods and prevent wasteful use of cloud resources.

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 for accounts once a threshold of spending has been reached.
7. Cloud usage MI should consider both software licensing, compute and storage costs.
8. Organisations should ensure that sufficient funds are available to cover licensing costs, and that controls are in place to prevent key services being shut down.

Considerations for Material Workloads

1. Monitoring of key services based on SLAs should be in place and regularly reviewed by the FI to identify usage anomalies, particularly where compound SLAs exist.
2. Protocols should be in place with the CSP to prevent cessation of services based on quotas being exceeded.

B) Design and Secure the Cloud

1. Cloud Architectural Reference Solutions & Practices

CSPs provide the FIs the ability to host their workloads in their cloud environment with a myriad of options to cater for diverse workloads and needs. As a result of the foreign nature of the cloud environment coupled with the availability of multiple implementation options, initial attempts to adopt the cloud services can be daunting to many.

To ease the cloud adoption journey many CSPs have developed cloud architecture reference solutions to help customer jumpstart their cloud implementation. These references are collections of solutions and design ideas to solve common cloud adoption problems.

Additionally due to the commoditized nature of cloud service consumption, the importance of architecting a standard catalogue of services which adhere to the business, technology and security standards of the FI is paramount.

Control Objectives

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

Considerations for Standard Workloads

1. It is recommended to use the FI's existing technology architecture governance to set standards and approve cloud patterns but the FI should leverage the CSP expertise for Cloud design patterns.
2. FIs should review business and technology requirements when developing cloud reference architectures. Business Requirement Documents (BRDs) and System Requirement Documents (SRDs) should be published and periodically reviewed.
3. Where end users are able to select and deploy these architectures directly an appropriate approval workflow should be in place.
4. A user role should exist which allows designated staff to develop and maintain cloud architectural patterns. Access rights to create non-standard architectures should be strictly controlled.
5. FIs may consider adopting the commonly available architectural references in the area of availability and resiliency, security, authentication, performance, operations and management.
6. The security architecture deployed in the Cloud environment takes into account the risks associated with Cloud connectivity, logical segregation and public access.

2. Virtualisation, Containerisation and DevOps

By its nature cloud is a distributed environment so 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, an FI should risk assess these in combination with other controls such as encryption or tokenisation.

In certain circumstances, such segregation may be bypassed or in the event of a system failure, data could be accessible 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.

Potential compromise of hardware, Operating System (OS) images or virtualisation management software such as hypervisors must be considered and managed.

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. This 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. Serverless is another offering that the CSPs are providing to FIs dynamically manage the allocation of systems to the workload processing requirements. The adoption of these new offerings combined with DevOps allows FIs to easily administer their Cloud environment in a more automated manner

DevOps is a hybrid of development and operations that is becoming more mainstream and the heart of agile development is to improve the quality of the software being delivered. It is also best suited developing and testing for security and vulnerabilities. There are various tools that can be used for DevOps and DevSecOps but it is up to the FIs to determine which one is best suited.

Control Objectives

- Manage the confidentiality and integrity risks associated with data co-mingling or shared tenancy environments.
- In the event of a software or hardware failure, 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 Standard Workloads

1. The 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 authorizing which ones are available for use.
2. 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.
3. The FI should carefully define its user access and authentication strategy, particularly for administrative users who have the ability to manage and change these fundamental tools supporting its cloud ecosystem.
4. The container images should contain a standard set of configurations that are designed and signed off 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. Ensure that changes to the container images are fully audited.
7. 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.
8. Security and vulnerabilities should be validated and tested using automation to perform testing.
9. Align any code deployment and configuration changes to the FIs change management process.

Considerations for Material Workloads

1. 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.
2. Integrity checks should be performed on container templates and any inconsistencies made detectable prior to use.
3. The FIs should have the appropriate checks to prevent production data being used during testing in non-production environments. The use of masked or synthetic data is strongly recommended.

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 centres 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 as power outages, fires, floods etc. Fault isolation is further implemented within each region to prevent the risk of contagion effect in an event of a fault or service outage.

Customers of the cloud services can choose to distribute their workload across multiple regions to improve the 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 Standard Workloads

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.

Considerations for Material Workloads

1. FIs should design their workload to leverage on available functionalities such as containerization and auto-scaling to automate the swift recovery of their services.
2. 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.
3. For workloads that are sensitive to latency FIs should implement the workload in the region that is closest to their customers or consider options to optimise customer experience (such as content delivery networks).
4. 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.
5. 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.
6. FIs should put in place a resumption plan for its critical services in an event of a total outage of cloud services. Some of the options that the FI cloud consider include implementing critical workload on two different CSPs or retention of on premise capabilities for added resiliency.

4. Network Architectures

Network architecture is a key consideration especially given the nature of 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
- Account for the use and adoption of cloud services to prevent shadow IT
- Ensure access to the cloud environment are granted on a need to basis
- Ensure that cloud work load is protected against network based attacks e.g. network intrusion attempts, application and DDoS attacks

Considerations for Standard Workloads

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. It is considered best practice for administrative interfaces to be on a segregated management network that is not accessible from the operational subnets.
3. Network access and security controls such as firewalls, IPS, advance threat protection and web proxy should be implemented to secure the on premise environment from the cloud.
4. The 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. VPN or direct network connection should be implemented to secure the traffic between the cloud and on premise environments where possible. IP source and destination restrictions should also be considered.
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.

Considerations for Material Workloads

1. Dedicated network connectivity should be implemented from the FI to the cloud environment, and remote administrator access to the cloud environment over the Internet should be restricted.
2. The controls in the cloud environment should be equivalent if not more secure than the FI's on premise environment.
3. Alternatively, FIs can consider rerouting the cloud traffic through the FIs' on premise environment to benefit from their existing on premise security controls.
4. FI should set up a dedicated security network segment to control all ingress and egress traffic from the cloud environment.
5. If possible Micro Segmentation to be considered with Software Defined Networks.
6. All internet traffic should be routed through a dedicated security network segment. All other network segments in the cloud environment should not have direct access to the Internet.

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 are critical to ensure that the information at rest are secure and the encrypted information, especially archival information, are accessible retrievable.

CSP environments typically offer a number of configurations for key management including a CSP managed option, an option to "Bring Your Own Key" where 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 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 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. The benefit of this model is that it 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 Standard Workloads

1. Keys should be rotated regularly in accordance with the industry best practices. Certificate revocation should also be tested from time to time.
2. Detailed policies and procedures should be in place to govern the lifecycle of cryptographic material from generation, storage, usage, revocation, expiration, renewal, to archival of cryptographic keys.
3. Backups of cryptographic material should be considered. These should 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.

Considerations for Material Workloads

1. FIs should generate their own unique cryptographic keys and secure the keys in the Cloud environment.
2. At minimum, the cloud based HSM should meet the FIPS and Common Criteria for cryptographic products.
3. Where encryption is used, the encryption keys should be stored separately from virtual images and information assets.
4. FIs may consider HSM as a service or deploying their own HSM for particularly critical workloads.
5. 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.
6. Offline storage in a suitably secure and fireproof environment should be considered for critical cryptographic material, the loss of which may materially impact the FI's ability to recover data or operate. This should be included in disaster recovery planning scenarios.
7. FIs should leverage on a FIPS 140-2 Level 3 validated HSMs to secure their cryptographic keys, and access to the HSM should be secured with multi-factor authentication.
8. Where possible, access to the HSM should be secured using multi-factor authentication.

6. Encryption

Controls for encryption and tokenisation can be used interchangeably and can be used in a complementary or stand-alone fashion depending on the solution.

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

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 a number of 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: 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 is less suitable for PaaS or SaaS environments, and can restrict the adoption of cloud services. There is also an associated cost, and in the event that 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 Standard Workloads

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 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 every day staff access.
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 should be drawn from the MAS Technology Risk Management Guidelines.

Considerations for Material Workloads

1. Stringent control should be exercised over cryptographic keys to ensure that secret keys are generated and managed securely, for instance within a Hardware Security Module (HSM).
2. 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.
3. If using a Content Delivery Network (CDNs) ensure there are appropriate controls in place for encryption key and certificate management. It is recommended that Extended Validation (EV) or Organisation Validation (OV) certificates are used to ensure robust organisational identity controls are in place. Secure certificate management protocols should also be considered.
4. 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.

7. Tokenisation

Controls for encryption and tokenisation can be used interchangeably and can be used in a complementary or stand-alone fashion depending on the solution.

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.

It is in the best interest of the FI to minimise its data footprint so as 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. 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 all 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 Standard Workloads

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 identify unique characteristics and all interactions and access to the sensitive data.
2. The Cloud service provider 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 should remain under the direct management of the FI.

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 must 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
- Permit user access only to the information assets they require to perform their role
- Ensure segregation of duties is in place for sensitive roles

Considerations for Standard Workloads

1. For each Cloud deployment there will be a master account. It is recommended only to use this account by exception.
2. Identity and Access management should be a 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 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. For end users, especially where corporate users are concerned, federation of Active Directory credentials could be used to allow an FI's existing processes and infrastructure to be leveraged.
5. Where federation 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 by the FI's technology architecture governance committee.
6. Where access is via the internet multi factor authentication and IP source restrictions are strongly recommended.
7. Where identity and access management assets reside in the cloud, strategies should be created and tested for migration or exit planning.
8. 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.
9. 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.
10. 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.
11. Access and usage of service, generic and administrator accounts should be controlled via appropriate privileged user access management controls and activities logged for review.
12. 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.

Considerations for Material Workloads

1. Multifactor authentication should be considered for user access to critical workloads.
2. 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.

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 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 have the ability to 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 for Standard Workloads

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 be subject to segregation of duties and separate from any user administrator function.
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. Multifactor authentication should be strongly considered for all privileged access.

Considerations for Material Workloads

1. There should be a mechanism in place to detect when unauthorised accounts are created that can access criticality rated information assets.
2. Multifactor authentication should be mandated for privileged access to material workloads.

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 for Standard Workloads

1. Detailed documentation of all systems remote access procedures including security controls management. This documentation should be regularly reviewed to ensure accuracy and currency.
2. All interfaces to cloud computing infrastructure should be consistent where possible so that remote access controls are uniformly controlled.
3. These interfaces should provide discrete segregated data flows to ensure that there is a secured and auditable method of accessing systems and data.
4. Remote access security measures such as two factor authentication, and Virtual Private Network (VPN) encryption should be implemented.
5. Where possible remote access network traffic should have defined source and destination.
6. 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.
7. 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.
8. All privileged remote access is to be reviewed for appropriateness by independent and qualified personnel.

Considerations for Material Workloads

1. FIs should implement a direct private connection from their data centre to the cloud environment, and restrict all direct remote access to the cloud environment over the Internet.
2. Where Internet access to the CSP cloud management console cannot be disabled, FIs should implement a complex passwords and multi-factor authentication for the login account. These accounts should be limited to emergencies only and not used to support day to day operations.
3. 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.
4. The FI should consider restricting access to certain parts of the network by remote access users. Jump boxes should also be considered for additional security.

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 and control both sanctioned and unsanctioned data transfers and access to the cloud services.

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 services
- Manage data processed and stored in the cloud environment in accordance to the FI's information security policy
- Permit users access only to information assets they require to perform their role
- Prevent unauthorized or unintended dissemination of data

Considerations for Standard Workloads

1. The FI should review their information asset classification framework to ensure that encompasses considerations for the cloud. The FI may wish to consider enhanced controls for high value information assets that reside in the cloud such as strong encryption, tokenization and logical segregation.
2. Where data in transit crosses cloud deployments content inspection technologies should be deployed to identify and, where appropriate, quarantine information assets that contain personally identifying information (PII) or customer information (CI). Policies containing the identification criteria should have defined owners and be subject to periodic review.
3. Where cloud services are accessible via the Internet, data loss prevention controls such as cloud access security broker should be implemented to monitor and control the access of the information.

Considerations for Material Workloads

1. The FI should perform periodic reviews of the users that are able to approve exceptions to DLP policies.
2. FIs should monitor the ingress and egress points for the use or adoption of unsanctioned cloud services or shadow IT to support internal business processes or operations.
3. Data loss prevention controls should be implemented to secure access from the internet to the cloud services, and control downloading and extraction of information from the cloud services.
4. 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.
5. FI should have a Data Loss Governance and risk management framework defined which should integrate with its capabilities in the cloud. Templates and patterns for sensitive data should be defined, and metrics regularly reviewed. An appropriate consequence management framework should also be defined and agreed between the CSP and the FI.

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 for Standard Workloads

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 controlled testing across the different environments
4. Access to source code repositories and privileged access to the development and testing environments are restricted to only specific authorized individuals.
5. Unencrypted customer data should not be used for testing in the Cloud environment. Test data must be de-personalised before it is transferred into the CSP's environment.
6. The processes supporting release management should ensure that source code which has been subjected to reviews (automated or manual) and cannot be tampered with by the author after it has been reviewed.
7. Automated source code applications should be regularly updated and reviewed to ensure currency and accuracy of their findings.

Considerations for Material Workloads

1. For source code relating to material systems it is recommended that enhanced reviews including manual source code review are performed.
2. The source code should be updated and tested regularly for new security and vulnerabilities.
3. Where source code is used for any material purposes, it is strongly recommended to perform a risk assessment to determine if it is necessary to compile binaries within the FI's own networks and copy the binaries into the Cloud. The recommendation is to compile on the FI's network and push the artefacts to the cloud.

13. Penetration Testing

Testing the security of applications and infrastructure provides assurance of the security posture of a service. Through the use of regular vulnerability assessments and 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 for Standard Workloads

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 of the systems involved in the provision of the service(s).

2. The tests should take into consideration 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 in order to have an understanding of 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.

Considerations for Material Workloads

1. 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.
2. PT scope should include application upstream and downstream dependencies, as well as any centralised release management or source code systems that the application utilises.

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 for Standard Workloads

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

Considerations for Material Workloads

1. 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.

2. 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.
3. 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.
4. FIs should consider the use of security analytics with machine learning capabilities to develop baseline to detect potential anomalies in the cloud environment.
5. The FIs should ensure that CSPs have snapshots of critical databases or systems of record for disaster recovery / business continuity.

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 for Standard Workloads

1. FI application development teams should ensure that no CID (Customer Identifiable data) 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.

Considerations for Material Workloads

1. 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.

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 in place controls that facilitate management, near real time capability to review any privileged activities to ensure they are in line with approved processes. Consideration should be given to Application, OS, Database and Network layers.

Where PaaS, or SaaS is used, the 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 controlled by the CSP for IaaS, PaaS and SaaS environments
- Ensure oversight of major changes that could impact the stability and/or security of the cloud operating environment.
- Detection of unauthorised or erroneous changes

Considerations / Standard workloads

1. Change management procedures should be mutually agreed between the CSP and the FI. Such procedures should be formalised, and include change request and approval procedures, as well as a reporting component.
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, conditions and scenarios that allow automated testing and releases should be defined. It is important to ensure that there is a full audit trail, record of the changes and evidence of pre-approval.

Considerations for Material Workloads

1. 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.
2. Change management governance should be incorporated into regular Service Level Management meetings.
3. FIs should review the change management procedures of the CSP, which should be independently assessed in line with OSPAR, SOC2 or other controls assessments.
4. 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.
5. FI should consider conducting post change testing where critical business functions may be impacted, including documented and evidenced test cases.

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 / Standard workloads

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 for consistent and secure creation of new servers.
5. Key environment changes should be monitored and automated alerts should be triggered to alert the security or the infrastructure team.
6. FIs should consider auto-remediation for high impact changes such as configuration of internet gateways or server images.

Considerations for Material Workloads

1. FIs should create environmental baselines, establish a process to review the baselines periodically, and monitor deviations from the baselines. These metrics should be reported at the Cloud governance forum and to appropriate service owners.
2. Where possible, FIs should implement auto-remediation to revert the environment to the baseline configurations where strict enforcement of the baselines is required.

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 Standard Workloads

1. FIs should ensure there is a framework for event categorization, impact, responsibility and the actions taken to address them.
2. 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.
3. Security and technology events and the various levels of severity should be appropriately defined and ownership agreed between the FI and the CSP.
4. FIs should consider the use of automated ticketing upon the detection of incident to improve turnaround for the response team.

Considerations for Material Workloads

1. 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.
2. 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.
3. 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 (i.e. Notice 644 Technology Risk Management)

Considerations for Standard Workloads

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 commonly 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 boards.

Considerations for Material Workloads

1. 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.
2. Appropriate security systems and measures, such as network intrusion detection/prevention systems (NIDPS), 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.
3. 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.
4. While it is recognized that it is usually the FI's responsibility to identify a relevant incident under Notice 644, 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 60m of receiving this 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.
5. 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 responsibility 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 / Standard workloads

1. The FIs should define a monitoring and metrics strategy with the CSP and leverage the monitoring capabilities provided by the CSP and define appropriate metrics for its applications.
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.

Considerations for Material Workloads

1. Automated increase for quotas for material workloads should be considered and thresholds regularly reviewed for appropriateness
2. The FIs need to ensure that business strategies and requirements, including special events such as index rebalancing, are taken into consideration when reviewing the capacity of their workloads.

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 engagements. 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 / Standard Workloads

1. FIs should maintain an inventory of the software used in the cloud environment, and track the vulnerabilities announced by the respective technology vendors.
2. The SW inventory should also be used to track software life cycle so that informed decisions can be made to replace or have mitigating controls.
3. Where possible, FIs should containerized their applications in the cloud environment to facilitate prompt patching while minimizing impact to the cloud workload.
4. The FI should work with the CSP and understand capabilities in their offerings that would help best with vulnerability and patching management.
5. The CSP should be able to demonstrate the status of their compliance with published vulnerabilities and their ability to patch when required.

Considerations for Material Workloads

1. FIs should conduct a periodic assessment to identify new vulnerabilities, and schedule the patching activities to remediate the vulnerabilities in accordance with their criticality.
2. 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.
3. The FIs should ensure that there is a robust process in place to review and remediate any vulnerabilities in a timely manner and prioritise over the vulnerabilities of standard workloads
4. An exception process needs to be created for any vulnerabilities that cannot be remediated.

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 time-frame required by the FI

Considerations for Standard Workloads

1. The CSP should develop disaster recovery and business continuity plans and where appropriate share the plans with the FI.
2. Ensure that all changes in the computing environment are reflected in the disaster recovery plan, and that all facilities are available.

3. There should be a communications plan or an automated call tree that covers both CSP and FI staff.
4. Ensure that the FI's crisis Management team is fully aware of the CSP's recovery plan.

Considerations for Material Workloads

1. 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.
2. 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.
3. CSPs should obtain necessary certifications for disaster recovery (e.g. ISO27001 and validated against ISO27018) and their processes should be audited by independent third parties with such audit reports made available to the FI.
4. When performing DR testing with the CSP, consider doing spot checks or testing on short notice to validate their level of readiness for an actual disaster event.
5. Ensure that any deficiencies noted during testing are recorded, and the implementation of corrective actions is monitored via the appropriate governance bodies.
6. Various disaster recovery scenarios including both component failure, full site loss and partial failures should be incorporated into the testing plan. These scenarios should be tested according to a strategy defined by the bank in line with its business continuity policy
7. 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 of time to validate operational stability.

Acknowledgements

The ABS Task Force Members:

1. ANZ Bank
2. DBS Bank
3. Credit Suisse
4. Singapore Exchange
5. Standard Chartered Bank
6. UBS

Checklist of considerations for standard and material workloads

S/N.	Control	Standard Workloads	Material Workloads
		(A) Govern the Cloud	
1.	**Organisational Considerations for the Management of CSPs**	1. A FI should design and implement a suitable governance body and roles, where appropriate with representatives of both the CSP and the FI. The governance body should be empowered to oversee adherence to SLAs, review KPIs and KRIs, incidents, security incidents and other relevant matters to the risks associated with outsourcing. This governance body should meet periodically, the frequency determined by the materiality of the arrangement. 2. It is recommended that metrics provide a complete view, both where controls are owned and operated by the FI or the CSP. Interfaces to internal governance bodies should also be considered for FI owned controls. 3. Execution of oversight of cloud outsourcing arrangements requires a specific skill-set. FIs should be mindful that when outsourcing that key staff and roles are identified and that their knowledge is kept up to date by training or other methods. 4. FIs should consider creating a specific role to execute oversight of cloud outsourcing arrangements. 5. 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. 6. Any incremental changes to outsourcing controls should be managed via the governance forum.	1. Where critical services have been outsourced representation on the governance body should be of appropriately senior technology and business representatives. 2. A single point of contact from the CSP should be formally identified and given a sufficient mandate. 3. A defined escalation procedure should be put in place for both the CSP and the FI to use.
2.	**Control Assessment & Monitoring**	1. Prior to embarking on any cloud outsourcing arrangement a thorough technical risk assessment of key controls should be performed based on the use cases. 2. Where possible an FI should ensure that a control failure triggers an automated response and notification. 3. The FI should consider leveraging the controls available in the cloud environment to enforce consistent security standards and baselines as well as automated remediation where possible.	1. FIs should assess their existing controls assurance framework for the suitability of managing cloud outsourcing. Key procedural controls must be identified, mapped and effectiveness thresholds defined. 2. Establish Management Information and dashboard material for reporting on control assessments. Define an appropriate oversight and escalation model to execute remediation activities which takes into consideration both FI and CSP owned activities. 3. FI should consider the use of analytics with machine learning (ML) and other best in breed technologies to develop baselines for compliance checks to highlight and avoid non-compliance.
4.	**Billing Models**	1. It is recommended that the FI have a centralised governance structure to manage master subscription and control how that is provisioned for specific workloads. 2. Ensure that all assets in the cloud are identified, have clear ownership assigned and are rated for their asset classification. 3. Do not use the CSP's master account to centrally manage the costs, create sub accounts which are aligned to the finance	1. Monitoring of key services based on SLAs should be in place and regularly reviewed by the FI to identify usage anomalies, particularly where compound SLAs exist. 2. Protocols should be in place with the CSP to prevent cessation of services based on quotas being exceeded.

		structure of the FI 4. Ensure there is training and educational material for users of the cloud environment which is tailored to help them understand the best adoption methods and prevent wasteful use of cloud resources. 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 for accounts once a threshold of spending has been reached 7. Cloud usage MI should consider both software licensing, compute and storage costs. 8. Organisations should ensure that sufficient funds are available to cover licensing costs, and that controls are in place to prevent key services being shut down.	

S/N.	Control	Standard Workloads	Material Workloads
(B) Design and Secure the Cloud			
1.	**Cloud Architectural Reference Solutions & Practices**	1. It is recommended to use the FI's existing technology architecture governance to set standards and approve cloud patterns but the FI should leverage the CSP expertise for Cloud design patterns. 2. FIs should review business and technology requirements when developing cloud reference architectures. Business Requirement Documents (BRDs) and System Requirement Documents (SRDs) should be published and periodically reviewed. 3. Where end users are able to select and deploy these architectures directly an appropriate approval workflow should be in place. 4. A user role should exist which allows designated staff to develop and maintain cloud architectural patterns. Access rights to create non-standard architectures should be strictly controlled. 5. FIs may consider adopting the commonly available architectural references in the area of availability and resiliency, security, authentication, performance, operations and management. 6. The security architecture deployed in the Cloud environment takes into account the risks associated with Cloud connectivity, logical segregation and public access.	
2.	**Virtualisation, Containerisation and DevOps**	1. The 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 authorizing which ones are available for use. 2. 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. 3. The FI should carefully define its user access and authentication strategy, particularly for administrative users who have the ability to manage and change these fundamental tools supporting its cloud ecosystem. 4. The container images should contain a standard set of configurations that are designed and signed off 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. Ensure that changes to the container images are fully audited.	1. 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. 2. Integrity checks should be performed on container templates and any inconsistencies made detectable prior to use. 3. The FIs should have the appropriate checks to prevent production data being used during testing in non-production environments. The use of masked or synthetic data is strongly recommended.

S/N.	Control	Standard Workloads	Material Workloads
		7. 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. 8. Security and vulnerabilities should be validated and tested using automation to perform testing. 9. Align any code deployment and configuration changes to the FIs change management process.	
3.	**Resiliency in Cloud Architectures**	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.	1. FIs should design their workload to leverage on available functionalities such as containerization and auto-scaling to automate the swift recovery of their services. 2. 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. 3. For workloads that are sensitive to latency FIs should implement the workload in the region that is closest to their customers or consider options to optimise customer experience (such as content delivery networks). 4. 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. 5. 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. 6. FIs should put in place a resumption plan for its critical services in an event of a total outage of cloud services. Some of the options that the FI cloud consider include implementing critical workload on two different CSPs or retention of on premise capabilities for added resiliency.
4.	**Network Architectures**	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. It is considered best practice for administrative interfaces to be on a segregated management network that is not accessible from the operational subnets. 3. Network access and security controls such as firewalls, IPS, advance threat protection and web proxy should be implemented to secure the on premise environment from the cloud. 4. The FI should have network access and	1. Dedicated network connectivity should be implemented from the FI to the cloud environment, and remote administrator access to the cloud environment over the Internet should be restricted. 2. The controls in the cloud environment should be equivalent if not more secure than the FI's on premise environment. 3. Alternatively, FIs can consider rerouting the cloud traffic through the FIs' on premise environment to benefit from their existing on premise security controls. 4. FI should set up a dedicated security network segment to control all ingress and egress traffic from the cloud environment. 5. If possible Micro Segmentation to be

S/N.	Control	Standard Workloads	Material Workloads
		advance threat protection controls implemented in the security network segment to filter and secure access to the cloud environment. 5. VPN or direct network connection should be implemented to secure the traffic between the cloud and on premise environments where possible. IP source and destination restrictions should also be considered. 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.	considered with Software Defined Networks. 6. All internet traffic should be routed through a dedicated security network segment. All other network segments in the cloud environment should not have direct access to the Internet.
5.	**Cryptographic Key Management**	1. Keys should be rotated regularly in accordance with the industry best practices. Certificate revocation should also be tested from time to time. 2. Detailed policies and procedures should be in place to govern the lifecycle of cryptographic material from generation, storage, usage, revocation, expiration, renewal, to archival of cryptographic keys. 3. Backups of cryptographic material should be considered. These should 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.	1. FIs should generate their own unique cryptographic keys and secure the keys in the Cloud environment. 2. At minimum, the cloud based HSM should meet the FIPS and Common Criteria for cryptographic products. 3. Where encryption is used, the encryption keys should be stored separately from virtual images and information assets. 4. FIs may consider HSM as a service or deploying their own HSM for particularly critical workloads. 5. 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. 6. Offline storage in a suitably secure and fireproof environment should be considered for critical cryptographic material, the loss of which may materially impact the FI's ability to recover data or operate. This should be included in disaster recovery planning scenarios. 7. FIs should leverage on a FIPS 140-2 Level 3 validated HSMs to secure their cryptographic keys, and access to the HSM should be secured with multi-factor authentication. 8. Where possible, access to the HSM should be secured using multi-factor authentication.

S/N.	Control	Standard Workloads	Material Workloads
6.	**Encryption**	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 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 every day staff access. 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 should be drawn from the MAS Technology Risk Management Guidelines.	1. Stringent control should be exercised over cryptographic keys to ensure that secret keys are generated and managed securely, for instance within a Hardware Security Module (HSM). 2. 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. 3. If using a Content Delivery Network (CDNs) ensure there are appropriate controls in place for encryption key and certificate management. It is recommended that Extended Validation (EV) or Organisation Validation (OV) certificates are used to ensure robust organisational identity controls are in place. Secure certificate management protocols should also be considered. 4. 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.
7.	**Tokenisation**	1. Careful risk assessment and evaluation should be performed on the tokenisation solution to identify unique characteristics and all interactions and access to the sensitive data. 2. The Cloud service provider 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 should remain under the direct management of the FI.	
8.	**User Access Management & Authentication**	1. For each Cloud deployment there will be a master account. It is recommended only to use this account by exception. 2. Identity and Access management should be a 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 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. For end users, especially where corporate users are concerned, federation of Active Directory credentials could be used to allow an FI's existing processes and infrastructure to be leveraged. 5. Where federation 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	1. Multifactor authentication should be considered for user access to critical workloads. 2. 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.

S/N.	Control	Standard Workloads	Material Workloads
		approved by the FI's technology architecture governance committee. 6. Where access is via the internet multi factor authentication and IP source restrictions are strongly recommended. 7. Where identity and access management assets reside in the cloud, strategies should be created and tested for migration or exit planning. 8. 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. 9. 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. 10. 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. 11. Access and usage of service, generic and administrator accounts should be controlled via appropriate privileged user access management controls and activities logged for review. 12. 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.	
9.	**Privileged User Access Management (PUAM)**	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 be subject to segregation of duties and separate from any user administrator function. 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. Multifactor authentication should be strongly considered for all privileged access.	1. There should be a mechanism in place to detect when unauthorised accounts are created that can access criticality rated information assets. 2. Multifactor authentication should be mandated for privileged access to material workloads.

S/N.	Control	Standard Workloads	Material Workloads
10.	**Administrative Remote Access**	1. Detailed documentation of all systems remote access procedures including security controls management. This documentation should be regularly reviewed to ensure accuracy and currency. 2. All interfaces to cloud computing infrastructure should be consistent where possible so that remote access controls are uniformly controlled. 3. These interfaces should provide discrete segregated data flows to ensure that there is a secured and auditable method of accessing systems and data. 4. Remote access security measures such as two factor authentication, and Virtual Private Network (VPN) encryption should be implemented. 5. Where possible remote access network traffic should have defined source and destination. 6. 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. 7. 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. 8. All privileged remote access is to be reviewed for appropriateness by independent and qualified personnel.	1. FIs should implement a direct private connection from their data centre to the cloud environment, and restrict all direct remote access to the cloud environment over the Internet. 2. Where Internet access to the CSP cloud management console cannot be disabled, FIs should implement a complex passwords and multi-factor authentication for the login account. These accounts should be limited to emergencies only and not used to support day to day operations. 3. 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. 4. The FI should consider restricting access to certain parts of the network by remote access users. Jump boxes should also be considered for additional security.
11.	**Data Loss Prevention**	1. The FI should review their information asset classification framework to ensure that encompasses considerations for the cloud. The FI may wish to consider enhanced controls for high value information assets that reside in the cloud such as strong encryption, tokenization and logical segregation. 2. Where data in transit crosses cloud deployments content inspection technologies should be deployed to identify and, where appropriate, quarantine information assets that contain personally identifying information (PII) or customer information (CI). Policies containing the identification criteria should have defined owners and be subject to periodic review. 3. Where cloud services are accessible via the Internet, data loss prevention controls such as cloud access security broker should be implemented to monitor and control the access of the information.	1. The FI should perform periodic reviews of the users that are able to approve exceptions to DLP policies. 2. FIs should monitor the ingress and egress points for the use or adoption of unsanctioned cloud services or shadow IT to support internal business processes or operations. 3. Data loss prevention controls should be implemented to secure access from the internet to the cloud services, and control downloading and extraction of information from the cloud services. 4. 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. 5. FI should have a Data Loss Governance and risk management framework defined which should integrate with its capabilities in the cloud. Templates and patterns for sensitive data should be defined, and metrics regularly reviewed. An appropriate consequence management framework should also be defined and agreed between the CSP and the FI.

S/N.	Control	Standard Workloads	Material Workloads
12.	**Source Code Reviews**	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 controlled testing across the different environments 4. Access to source code repositories and privileged access to the development and testing environments are restricted to only specific authorized individuals. 5. Unencrypted customer data should not be used for testing in the Cloud environment. Test data must be de-personalised before it is transferred into the CSP's environment. 6. The processes supporting release management should ensure that source code which has been subjected to reviews (automated or manual) and cannot be tampered with by the author after it has been reviewed. 7. Automated source code applications should be regularly updated and reviewed to ensure currency and accuracy of their findings.	1. For source code relating to material systems it is recommended that enhanced reviews including manual source code review are performed. 2. The source code should be updated and tested regularly for new security and vulnerabilities. 3. Where source code is used for any material purposes, it is strongly recommended to perform a risk assessment to determine if it is necessary to compile binaries within the FI's own networks and copy the binaries into the Cloud. The recommendation is to compile on the FI's network and push the artefacts to the cloud.
13.	**Penetration Testing**	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 of the systems involved in the provision of the service(s). 2. The tests should take into consideration 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 in order to have an understanding of 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	1. 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. 2. PT scope should include application upstream and downstream dependencies, as well as any centralised release management or source code systems that the application utilises.

S/N.	Control	Standard Workloads	Material Workloads
		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.	
14.	**Security Events Monitoring**	1. Secure and robust security logging infrastructure should be leveraged. Consolidation of logs to a centralized system should be in place to ensure that the integrity and availability of the logs are maintained. 2. The centralized log server should be secured and segregated from the operational environment to prevent unauthorized or accidental purging of the log information. 3. Logs should be streamed back to the FI for security incident and event correlation.	1. 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. 2. 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. 3. 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. 4. FIs should consider the use of security analytics with machine learning capabilities to develop baseline to detect potential anomalies in the cloud environment. 5. The FIs should ensure that CSPs have snapshots of critical databases or systems of record for disaster recovery / business continuity.
15.	**Securing Logs and Backup**	1. FI application development teams should ensure that no CID 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.	1. 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.

S/N.	Control	Standard Workloads	Material Workloads
		(C) Run the Cloud	
1.	**Change Management**	1. Change management procedures should be mutually agreed between the CSP and the FI. Such procedures should be formalised, and include change request and approval procedures, as well as a reporting component. 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, conditions and scenarios that allow automated testing and releases should be defined. It is important to ensure that there is a full audit trail, record of the changes and evidence of pre-approval.	1. 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. 2. Change management governance should be incorporated into regular Service Level Management meetings. 3. FIs should review the change management procedures of the CSP, which should be independently assessed in line with OSPAR, SOC2 or other controls assessments. 4. 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. 5. FI should consider conducting post change testing where critical business functions may be impacted, including documented and evidenced test cases.
2.	**Configuration Management**	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 for consistent and secure creation of new servers 5. Key environment changes should be monitored and automated alerts should be triggered to alert the security or the infrastructure team. 6. FIs should consider auto-remediation for high impact changes such as configuration of internet gateways or server images.	1. FIs should create environmental baselines, establish a process to review the baselines periodically, and monitor deviations from the baselines. These metrics should be reported at the Cloud governance forum and to appropriate service owners. 2. Where possible, FIs should implement auto-remediation to revert the environment to the baseline configurations where strict enforcement of the baselines is required.
3.	**Events Management**	1. FIs should ensure there is a framework for event categorization, impact, responsibility and the actions taken to address them. 2. 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. 3. Security and technology events and the	1. 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. 2. 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. 3. The FI should define playbooks for recovery

S/N.	Control	Standard Workloads	Material Workloads
		various levels of severity should be appropriately defined and ownership agreed between the FI and the CSP. 4. FIs should consider the use of automated ticketing upon the detection of incident to improve turnaround for the response team.	scenarios along with key roles and task ownership.
4.	**Incident & Problem Management**	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 commonly 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 boards.	1. 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. 2. Appropriate security systems and measures, such as network intrusion detection/prevention systems (NIDPS), 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. 3. 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. 4. While it is recognized that it is usually the FI's responsibility to identify a relevant incident under Notice 644, 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 60m of receiving this 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. 5. 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**	1. The FIs should define a monitoring and metrics strategy with the CSP and leverage the monitoring capabilities provided by the CSP and define appropriate metrics for its applications. 2. The FI's technology operations team should monitor and review capacity utilisation and	1. Automated increase for quotas for material workloads should be considered and thresholds regularly reviewed for appropriateness 2. The FIs need to ensure that business strategies and requirements, including special events such as index rebalancing, are taken

S/N.	Control	Standard Workloads	Material Workloads
		review where capacity may be at risk. Planning for upgrades, enhancements including funding requests should be regularly discussed in internal governance forums.	into consideration when reviewing the capacity of their workloads.
6.	**Patching and Vulnerability Management**	1. FIs should maintain an inventory of the software used in the cloud environment, and track the vulnerabilities announced by the respective technology vendors. 2. The SW inventory should also be used to track software life cycle so that informed decisions can be made to replace or have mitigating controls. 3. Where possible, FIs should containerized their applications in the cloud environment to facilitate prompt patching while minimizing impact to the cloud workload. 4. The FI should work with the CSP and understand capabilities in their offerings that would help best with vulnerability and patching management. 5. The CSP should be able to demonstrate the status of their compliance with published vulnerabilities and their ability to patch when required.	1. FIs should conduct a periodic assessment to identify new vulnerabilities, and schedule the patching activities to remediate the vulnerabilities in accordance with their criticality. 2. 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. 3. The FIs should ensure that there is a robust process in place to review and remediate any vulnerabilities in a timely manner and prioritise over the vulnerabilities of standard workloads 4. An exception process needs to be created for any vulnerabilities that cannot be remediated.
7.	**Collaborative Disaster Recovery Testing**	1. The CSP should develop disaster recovery and business continuity plans and where appropriate share the plans with the FI. 2. Ensure that all changes in the computing environment are reflected in the disaster recovery plan, and that all facilities are available. 3. There should be a communications plan or an automated call tree that covers both CSP and FI staff. 4. Ensure that the FI's crisis Management team is fully aware of the CSP's recovery plan.	1. 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. 2. 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. 3. CSPs should obtain necessary certifications for disaster recovery (e.g. ISO27001 and validated against ISO27018) and their processes should be audited by independent third parties with such audit reports made available to the FI. 4. When performing DR testing with the CSP, consider doing spot checks or testing on short notice to validate their level of readiness for an actual disaster event. 5. Ensure that any deficiencies noted during testing are recorded, and the implementation of corrective actions is monitored via the appropriate governance bodies. 6. Various disaster recovery scenarios including both component failure, full site loss and partial failures should be incorporated into the testing plan. These scenarios should be tested according to a strategy defined by the bank in line with its business continuity policy 7. 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

S/N.	Control	Standard Workloads	Material Workloads
			for an extended period of time to validate operational stability.