ABS Cloud Computing Implementation Guide 1.1

for the Financial Industry in Singapore

2 August 2016

Table of Contents

Section 1 : Introduction

Objective

The Association of Banks in Singapore (ABS) has developed this implementation guide for Financial Institutions (FIs) to use when entering into Cloud outsourcing arrangements.

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 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 information security controls in the Cloud must be at least as strong as what the FIs would have implemented had the operations been performed in-house should apply. In addition, the security controls should also address the unique risks that are associated with outsourcing to the Cloud.

These guidelines are set out in the three following sections:

- Section 2 addresses Information Asset 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 key controls recommended when entering into a Cloud outsourcing arrangement.

Definitions

This definition of Cloud is taken from the National Institute of Standards and Technology (NIST) available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

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

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.

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.

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

Deployment Models

Private cloud. The cloud infrastructure is provisioned for the exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

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 MAS Outsourcing Guidelines for further clarifications.

http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines%20Jul%202016.pdf

Section 2 : Outsourcing Classification

In this section, guidance is given as to what is likely to constitute material and non-material outsourcing in the context of cloud.

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 refer to Annex 2 of the MAS Outsourcing Guidelines July 2016.

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

Category	Factors influencing materiality
Likely to be material	• Use of unencrypted "customer information" that is referable to any named 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 risk management • Commercially sensitive contracts or data that could influence financial markets • Regulatory reporting or accounting data • Outsourced business activity is defined as critical by the FI
Likely to be non material	• Use "customer information" which is anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred • Staff data which does not include bank account or credit card data (e.g. information on name cards) • 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 Security Operations Centres, Cyber threat intelligence, • Development environments • Websites for accessing information that is classified as 'public'

The next section looks at the different scenarios where services may be provided in the cloud, and makes recommendations on the key controls that should be applied.

It is possible that the materiality of a Cloud outsourcing arrangement may differ per scenario. For instance, a data room may be used by one FI to store customer data, while another FI may use data room to store non-sensitive data.

Scenario	**Description**	**Typical Information Asset to be Protected**
Internet Banking or Payments portals	Applications involved in online banking functions such as account statements, bank transfers and payment processing. This specifically excludes systems of record (i.e. a general or account ledger) or core banking systems (i.e. CASA).	Banking information, customer information
Customer Relationship Management (CRM)	System used to manage a company's interactions with current and future customers. It is often used to organize, automate, and synchronize sales, marketing, customer service, and technical support.	Customer information (sometimes detailed information), customer history
Fraud prevention services	Whilst making transactions, third parties may be used to perform checks on credit card activity to identify and manage fraud.	Credit card information (PAN, Expiry, CVV, customer information, name, address)
Human Resources (HR) Portal	Portal for HR services potentially used for performing payroll, leave booking, appraisal or annual review and expenses	Employee information
Data Rooms	A portal where multiple parties (usually legal or commercial) review documents or product offerings.	Contract information, employee user information, logs
Service management	An application that collects request and incident ticket information and manages the request life-cycle	Incident tickets, change tickets, release management, internal configuration management, user information
Microsites	A microsite is an individual web page or a small cluster of pages which are meant to function as a discrete entity within an existing website or to complement an offline activity. The microsite's main landing page can have its own domain name or subdomain.	Potentially can have customer information, Client meta data. Also likely to have public information (high integrity, availability requirement)
Surveys	A website that contains a number of questions either to be used internally or externally. Some survey sites have login pages to save progress.	Limited Customer / employee / vendor information such as email address, name, password, meta data
Data Analytics	Operations to analyse or transform Data. Frequently requires ETL (Extract, Transform and Load) to facilitate the analysis	Customer information (sometimes sensitive information)
Email Security Products	Email Message Transport Agent hosted to review emails for remove spam or malicious code prior to being processed on companies mail servers	Sensitive emails (encrypted emails may not be read) email address metadata
Security Operations Centre (SOC)	Outsourced vendor providing a collective intelligence center that processes cyber threat intelligence and performs security orchestration	Internal Configuration information, device and systems logs, Incident information, employee information

Scenario	Description	Typical Information Asset to be Protected
Authentication Services	Two factor authentication services may require communication to external companies that may be located on cloud	Limited Customer / Employee / Vendor information such as username, encryption keys / customer mobile phone number
Testing	Environments used to perform testing. Can also include performance and volume testing	Source Code, configuration information, potentially masked production data
Development Operations (DevOps)	The use of a cloud environment for the purposes of software development	Source Code, compiled programs, configuration information
Content Delivery Networks (CDN)	These are typically Cloud arrangements which cache an FI's data and deliver content over a highly distributed and available network of servers	Varies. Networks can be used to deliver content which contains both public and customer data

1. Scenario Based Cloud Control Guidance Matrix

The below table links the various scenarios described above to recommended key controls described in Section 4 that can be deployed to increase the security of the cloud outsourcing arrangement.

Scenario	Controls										
	Encryption and / or Tokenisation	Dedicated equipment	Change Management and Privileged User Access Management (PUAM)	Virtualised Environment Security	User Access Management and Segregation of Duties	Collaborative Disaster Recovery Testing	Security Events Monitoring and Incident Management	Penetration testing & vulnerability analysis	Administrative Remote access	Secure System Development Life-cycle and Code Reviews	Securing log data and backups
Internet Banking or Payments portals	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	SR
Customer Relationship Management (CRM)	SR	D	SR	SR	SR	SR	SR	SR	SR	R	SR
Fraud prevention services	SR	D	SR	SR	SR	SR	SR	SR	SR	R	SR
HR Portal	SR	D	SR	SR	SR	SR	SR	SR	SR	R	SR
Data Rooms	SR	D	SR	SR	SR	D	SR	SR	SR	R	R
Service Management	SR	D	SR	SR	SR	SR	SR	SR	SR	R	R
Microsites	D	D	SR	SR	SR	D	SR	SR	SR	R	R
Surveys	D	D	SR	SR	SR	D	SR	SR	SR	R	D
Data Analytics	SR	D	SR	SR	SR	R	SR	SR	SR	R	R
Email Security Products	SR	D	SR	SR	SR	SR	SR	SR	SR	R	SR
Security Operations Centre (SOC)	SR	D	SR	SR	SR	SR	SR	SR	SR	R	SR
Authentication Services	SR	D	SR	SR	SR	SR	SR	SR	SR	R	SR
Testing	D	D	D	R	SR	D	R	SR	SR	D	R
Development Operations	D	D	D	R	SR	D	R	SR	SR	D	R
Content Delivery Networks	D	D	SR	SR	SR	SR	SR	SR	SR	D	R

LEGEND

Strongly Recommended	Recommended	FI Discretion
SR	R	D

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.

It is recognised 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 IT security are clearly understood, defined and contractually agreed before transferring any data into the cloud.

1. Contractual Considerations

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.

The FI should state the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices, including the circumstances under which each party has the right to change security requirements.

The FI should include contractual clauses limiting as far as possible, material changes to the service structure. The obligation of the CSP to notify the FI in the event such changes (including controls and location) are made should also be included. Specific regulatory requirements, such as the right to audit by the MAS, must also be included where possible.

Where a CSP elects to use subcontractors for any functions material to the provision of the Cloud service, the FI should ensure that it is notified and that the CSP remains accountable for the provision of service, and effectiveness of agreed controls including IT security controls. The CSP should also be responsible for managing their subcontractors directly.

Enforceable and measurable Service Level Agreements (SLAs) should be negotiated where possible, including 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.

Finally, the contract should clearly stipulate the situations in which both parties have a right to terminate the outsourcing arrangement. Typical examples of this could be a material change in the outsourcing arrangement or a failure of the CSP to notify the FI in the event of a significant security incident affecting the FI.

2. Data Centre

It is important to establish the city and country of the data centre(s) where data is processed and resides. 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.

A physical security risk assessment (commonly known as a Threat & Vulnerability Risk Assessment (TVRA)) should be conducted on data centres. The assessment should consider the types of threats faced by the site. This assessment is commonly undertaken by the CSP.

Common areas of assessment should include susceptibility to natural disasters, political and social risk, and the legal environment of the jurisdiction which the service provider will operate. For manpower resourcing, the availability of a competent workforce, and the CSP's on-boarding procedures including security screening should also be considered.

An appropriate policy to reduce the risk of data leakage in the data centre should be in place. All physical security controls as defined in the ABS Outsourced Service Provider Guidelines should be considered. These controls are available at:

http://abs.org.sg/docs/library/abs_outsource_guidelines.pdf

Due diligence of the CSP's data centre controls should cover all data centre locations that support the FI's processing and data storage requirements. It should not be assumed that controls are consistent across all locations.

Where it is not possible to perform on-site due diligence, an independent assessment report (e.g. SSAE16 SOC 2 / ISO 27001 / ISO 27018) should be provided by the CSP for all the data centres that process and store the FI's data. FIs will need to validate that the scope of the independent assessment meets the expectations defined in ABS Outsourced Service Provider Guidelines. A key part of the assessment must be a test of operational effectiveness of the controls put in place to protect the FI's data: generic assessments that review control design effectiveness are not sufficient.

Due diligence should be reviewed regularly, the frequency being determined by materiality of the outsourcing arrangement. It is particularly important to validate the on-going operational effectiveness of key controls.

3. Data Sovereignty

It is advised to consider the social, political and economic climate of a country before an FI places its data there. An FI should, in principle, enter into outsourcing arrangements only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements.

The FI and CSP should agree which countries the FI's data can reside in. A contractual clause requiring notification of any changes to these locations should be obtained. Any breach of this stipulation should trigger a right to terminate.

To ensure that data remains protected even if it leaves the jurisdiction of Singapore, it is recommended that FIs establish contractually binding requirements that require the CSP to notify the FI should the local legal requirements compel the CSP to disclose the data to a 3rd party. This will help to aid compliance to 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

4. Data Retention

An 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 unencrypted data in online or offline backups. Where data can be isolated or logically segregated this is simpler to manage. However in a shared environment, ensuring that unencrypted data is segregated by verified and appropriate technical means should be assessed as part of the due diligence process.

It is prudent for an FI to have an exit strategy in place and periodically validate the CSP's ability to restore service from backups. In standing up and breaking down suitable infrastructure to do so, the FI should ensure that its unencrypted data is securely removed and inaccessible to other customers of the CSP at all times.

For encrypted data, an 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 an FI does not have direct access to its data, an FI must also be able to compel the CSP to wipe all of its data and/or render it permanently inaccessible in a timely manner, particularly on any backup or distributed online media. Failing which, the obligation of the CSP to protect the FI's data should survive the expiry of the contract.

This can be challenging if the media is shared with other customers. A contractual commitment from the CSP to undertake such data deletion and protection is recommended.

5. 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.

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. Some of these are covered in other sections; however day to day management should be set out in an agreed procedure.

Key activities, inputs and outputs should be defined, along with accountabilities. The frequency and format of meetings to review key performance indicators (KPIs) and key risk indicators (KRIs) should also be defined. 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 assessment.

A Responsible-Accountable-Consulted-Informed (RACI) matrix is an industry accepted practice for this.

The CSP should have an outsourcing risk register in place, and should be able to demonstrate that internal governance exists to regularly review its risk profile and risk management decisions. These decisions should be shared with the FI if they are directly impacted by the risks.

Where SLAs are negotiated, these must be aligned with business requirements, and where possible enforceable penalty clauses included.

6. 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:

- Agreed procedure and tools used for deletion of data in a manner that data is rendered irrecoverable.
- 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.
- 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, financial institutions should ensure that the following are in place where appropriate:

- A legal agreement that commits the CSP to assist in the exit process. The agreement may also commit the service provider to support testing of the exit plan on an agreed frequency. These should include the format and manner in which data is to be returned to the FI, as well as contractually obligated support from the vendor. If the FI is using proprietary vendor software provided by the CSP, the data must remain usable should the contract be terminated.
- Data elements to be extracted and returned to the financial institution should be agreed upon at the start of the outsourcing arrangement and reviewed whenever there are material changes to the outsourcing arrangement.

7. Financial and Continuity Risk

A CSP should be reviewed for its financial and operational capabilities. These should include a check of its ongoing viability, as well as its ability to service its debt. Such a review should occur at least annually, and the outcome included when the FI reviews its exit plans.

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

This implementation guideline forms the minimum/baseline controls that CSPs should have in place. However, FIs with specific needs should liaise with their CSPs on a bilateral basis to implement any additional specific requirements.

1. Encryption

Controls for encryption and tokenisation can be used interchangeably, so they are combined in the guidance matrix 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.

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 / Good Practice

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

- Sensitive data including data backups should be subjected to appropriate encryption controls both in-motion and at-rest.
- 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.
- Detailed policies and procedures should be in place to govern the lifecycle of cryptographic keys from generation, storage, usage, revocation, expiration, renewal, to archival of cryptographic keys.
- 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).
- 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.
- 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.
- 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.

- 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.
- Encryption keys used for the encryption of FI data should be unique and not shared by other users of the cloud service.
- Other guidance on encryption requirements should be drawn from the MAS Technology Risk Management Guidelines.

2. Tokenisation

Controls for encryption and tokenisation can be used interchangeably, so they are combined in the guidance matrix 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 / Good Practice

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:

- 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.
- 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.
- Systems that perform tokenisation should remain under the direct management of the FI.

3. Dedicated equipment or 'Private Cloud'

By its nature cloud is a distributed environment, so this requirement is a key consideration when architecting a solution on Hybrid or Public Cloud infrastructure

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.

For situations where particularly sensitive information assets are used, an FI may consider dedicated equipment or a 'Private Cloud'.

Leveraging dedicated hardware also allows an FI to simplify the landscape for the location and control of its data.

Control Objectives

- Remove the confidentiality and integrity risks associated with data co-mingling or shared tenancy environments.
- Ensure that it is possible to track and manage the location of all FI information assets.
- Provide a high level of assurance that information assets can be accessed only by authorised individuals.
- In the event of a system failure, ensure that information assets cannot be accessed by error or malfeasance.
- Ensure that data is retained in accordance with FI data retention policies.

Considerations / Good Practice

- When planning private cloud architecture, ensure that all access to the environment is considered, this should include any CSP administrative access, as well as physical access controls.
- When planning private cloud architecture require that the CSP contractually guarantees dedicated hardware and its location.
- Review the backup locations of systems and data. Data residency requirements should be considered for all locations of sensitive FI data.
- Ensure that security monitoring controls provide assurance of the isolation of the environment.
- Gain assurance that firewall rules are effective, with particular attention to ingress and egress traffic.
- Ensure that assets are effectively managed and any system obsolescence is addressed.

4. Change Management and Privileged User Access Management (PUAM)

Where outsourcing is concerned, it is expected that the FI maintains effective control over their data. The CSP should have in place controls that facilitate management of privileged accounts, as well as 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 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 deep engagement between the FIs and the CSPs.

Control Objectives

- Ensure the confidentiality and integrity of FI's data.
- Ensure oversight of major changes that could impact the stability and security of the cloud operating environment.
- Manage change appropriately.
- Detect unauthorised or erroneous changes.

Considerations / Good Practice

- 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.
- Change management governance should be incorporated into regular Service Level Management meetings.
- Procedures for emergency and standard changes should be agreed, including the roles and responsibilities for change management.
- Users with privileged system access should be clearly defined and subject to regular user access reviews. It is recommended these should occur monthly.
- Privileged User access should be clearly tracked and reported, and be linked to an agreed and approved change request. Note it is not always necessary for the CSP to disclose change requests to the FI.
- All privileged user access should be monitored and peer reviewed in a timely manner. The speed with which this review occurs should be commensurate with the criticality of the information assets in the Cloud.
- The Privileged User Administration function should be subject to segregation of duties and separate from any user administrator function.

5. Virtualised Environment Security

As stated in the previous section, there are a number of scenarios where virtualisation can introduce new threat vectors to Cloud architectures. This is because such environments are sharing hardware between customers, and relying on logical and virtual controls to ensure data is segregated and secured.

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

Control Objectives

- Ensure the confidentiality and integrity of data in a virtualised cloud architecture.
- In the event of a software or hardware failure, ensure that information assets remain secure or are securely removed.

Considerations / Good Practice

- Virtual images should be thoroughly penetration tested.
- Virtual Images should have controls in place to provide assurance of their integrity.
- Administrative interfaces should be on a segregated management network that is not accessible from the operational subnets.
- Where encryption is used, the encryption keys should be stored separately from virtual images and information assets.
- Security monitoring should be in place to detect and provide early warning of any compromises.

6. User Access Management and Segregation of Duties

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 identify and access management requirements, approval, provisioning, credential management, access review and revocation.

Control Objectives

- Ensure the confidentiality and integrity of FI's data.
- Permit users access only to the information assets they require to perform their role.
- Ensure segregation of duties is in place for sensitive roles.

Considerations / Good Practice

- 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.
- An FI's Identity and Access management policies and standards should be applied in full in the CSP environments used by the FI to ensure consistency.
- 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.
- 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.
- 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.
- Access and usage of service, generic and administrator accounts should be controlled via appropriate privileged user access management controls and activities logged for review.
- 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.

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 accuracy, completeness, and validity of recovery procedures.
- Verify the capabilities of the personnel executing the recovery procedures.
- Validate the accuracy of the information in the disaster recovery plan.
- Verify that the time estimates for recovery are realistic.
- Ensure that all changes in the computing environment are reflected in the disaster recovery plan, and that all facilities are available.

Considerations / Good Practice

- The CSP should develop disaster recovery and business continuity plans and share the plans with the FI.
- CSPs should obtain necessary certifications (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.
- Put in place a communications plan or an automated call tree that covers both CSP and FI staff.
- Ensure that the FI's Crisis Management team is fully aware of the CSP's recovery plan.
- 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.
- Ensure that any deficiencies noted during testing are recorded, and the implementation of corrective actions is monitored via the service management meetings.

8. Security Events Monitoring and Incident Management

Cyber-attacks and the compromise of a computer system 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.

Timely detection of security incidents coupled with tight integration with incident response and management processes can allow security incidents to be remediated speedily, thereby limiting potential damages.

Control Objectives:

- Provide early detection of network and system anomalies in the IT environment to facilitate timely response to potentially developing security incidents.
- 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 security incidents are appropriately escalated and notified to the relevant stakeholders.

Considerations / Good Practice

- Appropriate detection mechanisms should be in place at the network, system, and application level to analyse activities that could affect the security and stability of the cloud service.
- 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.
- 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.
- Secure and robust security logging infrastructure such as consolidation of logs to an independent system should be in place to ensure that the integrity and availability of the logs are maintained.
- 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.
- Based on the materiality of the outsourcing arrangement, a Security Operations Centre (SOC) operating on a 24x7 basis should be strongly recommended to provide active monitoring of security events and timely escalation of security incidents.
- 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.
- Definition of a security incident and the various levels of severity should be appropriately defined and agreed between the FI and the cloud service provider.
- Criteria and performance requirement i.e. SLA for the escalation, notification, containment, and closure of relevant security incident should be appropriately defined and agreed between the FI and the CSP.
- Review and testing of the security incident response plan should be conducted on a regular basis by the CSP and involve the FI where appropriate.
- Access to appropriate reports on relevant security 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.

9. Penetration Testing & Vulnerability Management

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.

Vulnerability Assessment and Penetration Testing (VA/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 VA testing that can be conducted.

Please refer to the ABS guidelines of Penetration Testing for further details, which can be found here:

http://abs.org.sg/docs/default-source/default-document-library/abs-pen-test-guidelines.pdf

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 / Good Practice

- 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).
- The tests should take into consideration threats that are unique to cloud computing, such as hypervisor jumping and weak application program interfaces.
- Testers should be aware of typically 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.
- FIs should engage the CSP prior to engaging VA/PT to understand any technical limitations of testing.
- All vulnerabilities should be risk assessed, tracked and managed / treated appropriately.
- Where a CSP is responsible for remediation of identified vulnerabilities this should occur in line with any SLA / timeframe agreed in the contract.

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 / Good Practice

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

Examples

Consider a microsite that is hosted by a CSP that is providing infrastructure as a service. From the CSP's point of view there should be strong authentication for the access to the network infrastructure / hypervisor / storage as applicable. There is likely to be a platform to manage changes to the infrastructure – adding / removing systems, assigning storage, changing network setup. Finally the systems (Operating Systems, Databases, Application interfaces) themselves require secure remote access (if used).

Consider a CRM platform as a service hosted by a CSP where the FI only has access to an administration portal. An FI should consider reviewing the remote access controls of the CSP (and any third parties) to the administration portal.

11. Secure Software Development Life-cycle and Code Reviews

With the emergence of cloud computing, an increasingly greater number of applications are being built on cloud platforms. Cloud service development requires a different approach than the traditional software development life-cycle (SDLC) as the applications are no longer deployed on an on-premises infrastructure with implicit security, compliance, control, operational transparency and perceived service level requirements.

Secure SDLC methodology puts emphasis on incorporating security methodology into the SDLC phases.

Above and beyond the typical secure SDLC, the secure SDLC methodology for cloud applications requires explicit consideration of the integrity of code artefacts and of environments where applications are developed and tested throughout each development iteration. Secure destruction of data and a clean breakdown of environments must also be considered.

Control Objectives:

- Ensure operational embedding of risk assessment, threat modelling, vulnerability assessment, security testing, configuration review, remediation and security improvement processes in the cloud application SDLC methodology.
- Ensure that development and testing environments are protected from unauthorized access.
- Ensure confidentiality and integrity of source codes, other code artefacts (e.g. compiled codes, libraries, runtime modules) and system configuration in all environments.
- Prevent inappropriate removal of code artefacts and system configurations from the underlying systems of the development and testing environments.
- Ensure timely removal of code artefacts and system configurations during environment tear-down at the end of each development iteration.

Considerations / Good Practice

- Content version controls, and strict processes for the migration of source code from one environment to another must be clearly defined as part of a release management process.
- Segregation of duties should be in place for code deployment.
- Access to source code repositories and privileged access to the development and testing environments are restricted to only specific authorized individuals.
- Unencrypted production data should not be used for testing in the Cloud environment. Test data must be depersonalised before it is transferred into the CSP's environment.
- Operating System images for environments should be strictly controlled.
- 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.

12. 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 confidentiality of backup data.
- Ensure that sensitive data stored in backups is wholly identifiable and can be securely deleted.

Considerations / Good Practice

- FIs should work with CSPs to understand the logging capabilities of the service in order to gain assurance that there is no "unexpected" logging of data.
- Establish requirements for forensic investigation including how to ensure that log data can be acquired in a forensically sound manner.
- Appropriate access control must be in place for backups and log data.
- FIs should consider the contents of backups and encrypt sensitive data where appropriate.
- FIs should give due consideration to the management of encryption keys used for backup purposes.
- The capability to recover data in a usable form should be regularly tested. Such restoration tests must be conducted securely to minimise any risk of data leakage.

Acknowledgements

The ABS Task Force Members:

1. ANZ Bank
2. Barclays Bank
3. DBS
4. Deutsche Bank
5. HSBC
6. OCBC
7. Singapore Exchange
8. Standard Chartered Bank
9. UOB