Introduction to the Cloud Decision Framework

Why this framework is needed?

Cloud Computing is poised to transform how Government and BFSI Industry uses information technology. However, this transformation can only come about if the industry is confident that the use of Cloud Computing will not interfere with legal obligations and sound business practice.

This document has been created after understating the requirements and challenges from Government and BFSI Companies, Cloud Service Providers (CSP), Consulting organizations, BFSI Regulators and industry bodies. It proposes Cloud Decision Framework in the form of a unified, condensed and clarified set of best practices to help Government and BFSI companies to focus on and navigate through the relevant regulatory issues when contemplating a move to the cloud. The Cloud Decision Framework covers key requirements such as confidentiality, availability and integrity and is derived from the very laws, regulations and guidelines with which the Government and BFSI companies must comply.

The configuration of Cloud Services will vary greatly from CSP to CSP and not all solutions will be able to meet the Cloud Decision Framework. It is the Government and BFSI Companies’ obligation to ensure that the Cloud Services they use are compliant. The Cloud Decision Framework will help the Government organizations and BFSI to be better prepared, have a clearer understanding of the relevant requirements and to make the right decisions.

Whom is the framework for?

The Government and BFSI Companies

The Cloud Decision Framework focuses on the regulations applicable to Government and BFSI companies, being subject to some of the most stringent requirements. However, the definition of a Government and BFSI Company is broad. The term may encompass different kinds of organizations that deal with the insurance companies, such as general, life, re-insurance companies and brokers. Although this note focuses on Government and BFSI companies, this Cloud Decision Framework should still be broadly consistent and applicable for the whole industry. However, recognising that the Cloud Decision Framework are broad statements of regulatory requirements, all Government and BFSI companies will, of course, need to obtain their own legal advice in relation to their intended use of Cloud Services. In some countries, for example, BFSI companies may need to consult with or obtain approval from BFSI Regulators in order to use a Cloud Service. In addition, Government organizations may be subject to separate laws and regulations. By complying with this framework, Government and BFSI companies will have addressed the overarching key concerns with and challenges of using Cloud Services in the Government and BFSI.
**Cloud Service Providers**
When designing or contracting to provide Cloud Services, referring to the Cloud Decision Framework will help CSPs better understand and meet the regulatory issues that their Government and BFSI Company customers face.

**Consulting Organization**
Consulting organizations can use, endorse or recommend the Cloud Decision Framework as helpful guidance for the Government and BFSI companies or CSPs that they represent.

**Industry Bodies**
Industry Bodies can use, endorse or recommend the Cloud Decision Framework as helpful guidance for the Government and BFSI companies or CSPs that they represent.

**Government and BFSI Regulators**
Government and BFSI Regulators can use, endorse or recommend the Cloud Decision Framework as “Best Practices” and additional guidance for the Government and BFSI companies that they regulate (as the Cloud Decision Framework have been developed to capture the broad principles underlying regulation).

**How is the Cloud Decision Framework structured?**
The Cloud Decision Framework is based on 10 Principles for adopting cloud. For each of the ten principles there is:
(i) a summary explanation of what the principle means in practice for Government and BFSI Companies
(ii) a checklist for Government and BFSI companies to follow in order to meet the principle
(iii) a list of the key laws, regulations, and guidelines that underpin the principle in four of the key jurisdictions in the Asia Pacific region – India, Singapore, Hong Kong and Australia (applicable as of November 2013).

The Cloud Decision Framework is broadly consistent and applicable across the Asia Pacific region although some variations will apply.
What are Cloud Services?

Cloud Computing or Cloud Services means on demand network access to a shared pool of configurable computing resources. In other words, Cloud Services provide customers with on demand access, using a network connection, to information technology or software services, all of which the CSP can configure to the needs of the customer.

Service Models
There are three common delivery models for Cloud Services:
(i) Infrastructure as a Service (IaaS), where the CSP delivers IT infrastructure e.g. storage space or computing power
(ii) Platform as a Service (PaaS), where the CSP provides a computing platform for customers to develop and run their own applications
(iii) Software as a Service (SaaS), where the CSP makes available software applications to customers.

Deployment Models
There are four common deployment models for Cloud Services, each characterized according to:
(i) who manages the day-to-day governance, operation, security and compliance of the service
(ii) who controls the infrastructure (including physical infrastructure such as facilities, computers, networks and storage equipment)
(iii) where the infrastructure is located
(iv) who can access the Data being hosted.

They are:
Streamlined Cloud with infrastructure controlled and managed sometimes by the customer, but more often by a CSP. The infrastructure is located either on customer premises or, again more typically, on the CSP’s premises. In all cases, the Data and services are accessible exclusively by the particular customer.

Public Cloud with infrastructure controlled and managed by the CSP and located off-premise from the customer. Although the Data and services are protected from unauthorised access, the infrastructure is accessible by a variety of customers. Public Cloud is also referred to as a ‘multi-tenant solution’ because there are multiple customers who will all have access to the same infrastructure.
**Community Cloud** serves members of a community of customers with similar computing needs or requirements, such as security, reliability and resiliency. The infrastructure may be controlled and managed by members of the community or by a CSP. The infrastructure is located either on customer premises or on the CSP’s premises. The Data and services are accessible only by the community of customers. Community Cloud is by its nature a ‘multi-tenanted solution’ because there are multiple members of a community of customers who will all have access to the same infrastructure.

**Hybrid Cloud** is a combination of two or more of Private Cloud, Public Cloud or Community Cloud. Hybrid Cloud infrastructure can be owned and managed by the customer or by a CSP, and in either case the infrastructure may be located on-premise or off-premise, or both (e.g. some on-premise Private Cloud integrated with off-premise Community Cloud or Public Cloud). The Data and services can be accessed based on the design of the solution, corresponding to whether the architecture has public, private or community characteristics. It can however also provide a ‘dedicated’ solution or component.

All four deployment models are capable of meeting the Cloud Decision Framework requirements. However, it is essential that Government and BFSI companies looking at Public Cloud, Community Cloud or Hybrid Cloud models that are multi-tenanted only engage CSPs who offer a model that can host multiple tenants in a **highly secure way**, so that data storage and processing for each tenant is **segregated**. If not then the Cloud Services will not meet these Cloud Decision Framework, in particular Principle 8.

**What are the key challenges with Cloud Services for the Government and Financial Institutions?**

Government and BFSI companies are stringently regulated. This is because Government and BFSI Regulators are committed to maintaining an organization that is safe, stable and secure.

Contrary to common misconceptions, Government and BFSI Regulators in the Asia Pacific region do not prohibit the use of Cloud Services per se and do recognise that they are an increasingly important option for Government and BFSI Companies’ technical infrastructure and budget management. However, Government and BFSI Regulators are compelled to oversee that any implementation of Cloud Services is undertaken with appropriate due care and attention. Correspondingly, Government and BFSI companies need to approach Cloud Services with a high degree of sensitivity to ensure regulatory compliance, often across multiple jurisdictions.

In terms of the regulatory framework for Cloud Services, most Government and BFSI Regulators have not published specific Cloud Service guidelines. Instead, they tend to rely on existing regulations and guidelines on outsourcing, data risk management, technology risk management and business continuity management.

Despite differences in the presentation of regulatory requirements and the approach of different Government and BFSI Regulators, the following common conditions emerge which are imposed across all Government and BFSI Companies, regardless of jurisdiction and have particular resonance for Cloud Services:
• The importance of Government and BFSI companies maintaining control over their activities and Data (see Principle 2).
• The ability for Government and BFSI companies and applicable Government and BFSI Regulators to audit the CSP (see Principle 3).
• Ensuring Government and BFSI Companies’ Data, particularly Customer Data, is kept in strict confidence (see Principle 4) and is not kept for any other purpose than providing the service (see Principle 7).
• Prescriptive security requirements (see Principle 4).
• Transparency about the exact location of the Government and BFSI Companies’ Data (see Principle 6).
• The need for segregation of Government and BFSI Company Customer Data (see Principle 8).

In addition to FSI specific rules and guidance, in most jurisdictions other general legal requirements will also be relevant and therefore feature in the Cloud Decision Framework. These include Privacy Regulations, which, for example, impose requirements that apply in respect of any Personal Data that may be stored, processed or hosted by the CSP (e.g. security, consents, transfers of Personal Data and, in some countries, additional rules related to security breach and notification). Government and BFSI companies will also need to consider, in particular, the impact of any general statutes, regulations or common law relating to confidential information, law enforcement or judicial access to Data.
1. Service Provider Reputation and Competence
2. Review, Monitoring and Control
3. Audit
4. Confidentiality and Certified Security Standards
5. Resilience and Business Continuity
6. Data Location and Transparency
7. Limits an Data Use
8. Data Segregation/isolation
9. Conditions an Subcontracting
10. Conditions an Termination

Key:

- India
- Singapore
- Hong Kong
- Australia
Service Provider Reputation and Competence

Government and BFSI companies must carry out, and CSPs must assist in facilitating, a risk assessment and due diligence on the CSP to ensure that the CSP and its Cloud Services meet the legal, regulatory, contractual and business requirements. Government and BFSI companies should have in place a risk management plan that includes measures to address the risks associated with the use of Cloud Services.

There is a variety of deployment models for Cloud Services. As part of the due diligence process, Government and BFSI companies should ensure that they understand the pros and cons of each deployment model and the specific configuration being proposed by the CSP to determine whether it is suitable for their purposes and can meet its regulatory requirements.

Most Government and BFSI Regulators require Government and BFSI companies to carry out impact assessments prior to entering into the contract for Cloud Services, but this is also sound business practice. Some Government and BFSI Regulators have a more detailed process – for example the Monetary Authority of Singapore, who has a specific detailed questionnaire document that must be completed by the Government and BFSI Company.

**Government and BFSI Company Checklist:**

- Evaluate the CSP. Does it have the requisite experience, competence, financial strength, resources and business reputation? Have you investigated any existing complaints/litigation?

- Carry out due diligence to ensure that the CSP can comply with these Principles. You may wish to run through each of these Principles with the CSP and ask it to demonstrate how it will comply with them.

- If the results of the due diligence show deficiencies against the legal, regulatory or business requirements, these deficiencies must be addressed **prior to** entering into the contract with the CSP or another CSP must be engaged.

- Require the CSP to assist in the due diligence process. A reputable CSP should be willing and able to provide answers to all your questions and be familiar with the specific regulatory requirements that you must meet.

- Complete the relevant Government and BFSI Regulator’s questionnaire or other review process. A good CSP should be able to help you with this process.
Examples of regulations and guidelines that underpin this principle:

- IRDA Guidelines para 9.1, 10
- IDRBT Cloud Security Framework Chapter 3, p9
- MAS Outsourcing Guidelines Para 6.2
- MAS Outsourcing Guidelines Para 6.3
- MAS TRM Guidelines Para 5.1
- MAS TRM Guidelines Para 5.2
- MAS Outsourcing Questionnaire
- MAS Banking Secrecy Notice
- HKMA Outsourcing Guidelines Para 2.2
- HKMA Outsourcing Guidelines Para 2.3
- APRA Outsourcing Standard Para 22
- APRA Outsourcing Guide

Review, Monitoring and Control

Compliance does not end at signature of the contract. CSPs must provide regular reporting and information to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the contract. Government and BFSI companies and CSPs must meet regularly to review the reports and performance levels. The contract must provide for an effective mechanism for remedial actions arising from any issues that emerge or non-compliance.

This principle goes towards maintaining stability in the industry and ensuring that Government and BFSI Companies’ and CSPs’ responsibilities do not end at the point that a contract is signed but that Government and BFSI companies continue to be vigilant in compliance throughout the contract lifecycle. Government and BFSI Regulators recognise that Government and BFSI companies may need to outsource certain services, but they make it clear that Government and BFSI companies cannot outsource their primary responsibility for risk and compliance.

CSPs should regularly (e.g. annually) provide Government and BFSI companies with copies of independent third party audit results that the CSP has obtained, e.g. SSAE 16 SOC1 (Type II) reports. CSPs should also provide copies of reports of penetration testing that the CSP has carried out or arranged to be carried out by independent third parties (which will help to support Principle 4).
☑️ Government and BFSI Company Checklist:

• Has the CSP given you a full overview of the testing, review and audits that it conducts on a regular basis? Look for a CSP who is prepared to have their processes verified and be willing to share independent third party audit results and penetration testing.

• Does the CSP agree to make available to you copies of its independent audit reports? SSAE16 SOC 1 (Type II) reports are a good one to ask for.

• Ensure that the CSP also provides you with real-time and continuous information about the current availability of the services, history of availability status, details about service disruptions and outages and scheduled maintenance times.

• Does the CSP provide you with access to a dedicated account manager in order to assist in the management of performance and problems?

• Does your contract include provision for escalation of issues that arise from the audit and review process or the ability to participate in the CSP’s product compliance program if they have one?

Examples of regulations and guidelines that underpin this principle:

- IRDA Guidelines, para 9.3,11.2
- MAS Outsourcing Guidelines, Para 6.7
- MAS TRM Guidelines, Para 5
- MAS Outsourcing Questionnaire
- HKMA Outsourcing Guidelines, Para 2.1
- HKMA Outsourcing Guidelines, Para 2.6
- Banking Ordinance, Seventh Principle
- APRA Outsourcing Standard, Paras 17 and 37
- APRA Outsourcing Guide

CSPs must provide Government and BFSI companies and applicable Government and BFSI Regulators with audit rights.

In addition to the monitoring, regular reviews and independent reports (set out in Principle 2), most Government and BFSI Regulators require that CSPs allow the Government and BFSI Regulator and, at times, the Government and BFSI Company rights to carry out an inspection of the CSP. This will enable the Government and BFSI Regulator and Government and BFSI Company to confirm that CSPs are complying
with the requirements set out in this Cloud Decision Framework and with contractual and business requirements of the Government and BFSI Company, rather than just relying on the information provided by the CSP.

**Government and BFSI Company Checklist:**

- Do you have a contractual commitment from the CSP to allow audits by you and the applicable Government and BFSI Regulators where required? Avoid a CSP who does not provide audit rights for the Government and BFSI Company and applicable Government and BFSI Regulators.
- Check the scope of the audit right provided. It should cover audits of the CSP’s facilities, systems, processes and data relating to the services.
- To ensure that any audit can be undertaken, the CSP must tell you the exact location of its data centers and exactly where your Data is hosted (see also Principle 6).

**Examples of regulations and guidelines that underpin this principle:**

- IRDA Guidelines para 9.9(iii)
- IT Act Rules 2011
- IDRBT Cloud Security Framework – Chapter 3, page 13
- MAS Outsourcing Guidelines, Para 6.8
- MAS Banking Secrecy Notice
- MAS Outsourcing Questionnaire
- HKMA Outsourcing Guidelines, Para 2.8
- APRA Outsourcing Standard, Para 30
Confidentiality And Certified Security Standards

CSPs must be certified to have and maintain robust security measures and comprehensive security policies that meet or exceed international standards (ISO27001 accreditation should be a minimum). CSPs should use encryption technology that meets or exceeds international standards to protect and secure the Government and BFSI Companies’ Data at all times.

Government and BFSI Regulators understandably place a lot of emphasis on confidentiality and security, since this will protect Government and BFSI Companies’ reputation and maintain high levels of customer confidence. This principle is also important to Government and BFSI Regulators because it helps to combat the increase in cyber security threats that can have a material business impact. Therefore, Government and BFSI Regulators require Government and BFSI companies to place strict security requirements on CSPs.

Certification is an important benchmark used by Government and BFSI Regulators in measuring security standards. There is currently no one recognized industry certification specifically for Cloud Services. However, ISO27001 is generally considered the most appropriate certification given the high benchmark that CSPs must meet to achieve and maintain it. Other CSP certifications, whilst not specifically relevant to Government and BFSI Companies, can be indicative of industry best practice and should also be taken into consideration (e.g. if the CSP has been granted authority under FISMA (the US Federal Information Security Management Act) or is HIPAA compliant).

In India, the IT Act Rules specifically call out ISO27001 certification as an example of “Reasonable Security Practices”

To help potential customers of Cloud Services evaluate different CSPs, the Cloud Security Alliance (a not-for-profit organization) has developed a set of security and privacy criteria called the Cloud Control Matrix (CCM). Customers can use it to compare different CSPs’ data controls. Government and BFSI companies should use CSPs who meet the requirements set out in the CCM.

In many countries, in addition to financial services regulations and guidance, maintaining confidentiality is also a legal requirement imposed by statute and/or by case law and again, certification is a useful tool to meet this. Privacy Regulations also require organizations to maintain high levels of security in respect of Personal Data in order to ensure that the privacy of individuals is safeguarded and Personal Data does not get into the wrong hands.

Government and BFSI Company Checklist:

- Is the CSP ISO27001 certified?
- Is the CSP able to meet other recognized industry security standards, for example, those in relation to
FISMA and HIPAA? This will provide a useful indicator to the robustness of the systems and the competence of the CSP.

- What commitments has the CSP given in relation to its security provisions beyond certification? Commitments should usually cover 24-hour monitoring of physical hardware, secure networks, encryption of Data in transit and encryption of the hardware used to host the Data. Look for a CSP that uses Advanced Encryption Standard encryption.

- Have you checked the CSP and its security commitments against the CCM criteria?

- Does the CSP conduct penetration tests to enable continuous improvement of incident response procedures? Ask for an explanation as to the testing and frequency of testing in this respect.

**Examples of regulations and guidelines that underpin this principle:**

- IRDA Guidelines, para 9.11
- IT Act Rules 2011 rule 4(v), rule 8(2)
- IDRBT Cloud Security Framework, Chapter 3, p 13, 14
- MAS Outsourcing Guidelines, Para 6.5
- MAS TRM Guidelines
- Banking Act, Section 47
- MAS Banking Secrecy Notice
- MAS Outsourcing Questionnaire
- PDPA, Section 24
- HKMA Outsourcing Guidelines, Para 2.5
- HKMA Technology Guidelines
- PDPO, Schedule 1, Data Protection Principles, 4
- APRA Outsourcing Standard, Paras 21 and 41
- APRA Data Risk Guide
- APRA Security Guide

---

**Resilience And Business Continuity**

The Cloud Service must be reliable. CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives and with regularly tested and updated procedures and systems in place to meet those objectives. The risks of downtime should be minimized through good planning and a high degree of system resilience.

This principle is important to Government and BFSI Regulators as service disruptions in the FSI can have a significant impact on the wider community. Government and BFSI Regulators recognise that service disruptions can happen but require that the risk of them arising and their effect be minimized.
through having in place appropriate business continuity plans and procedures. Government and BFSI companies must ensure such plans and procedures are in place and regularly tested and updated to protect against service disruption.

**Government and BFSI Company Checklist:**

- Have you reviewed the CSP’s track record on service continuity (e.g. over the past five years)? Is the CSP able to demonstrate that consistently high levels of service availability have been obtained?

- Does the CSP give a tangible commitment to high availability of service? A commitment to uptime of 99.9% is a good measure (measured as the number of minutes the service is available in a month as a percentage of the total number of minutes in that month). You should also look for a CSP that financially backs up this commitment in terms of consequences of failure to meet it.

- Check that the CSP has an “active-active” configuration i.e. if a failure occurs in one server or data center, another server or data centre can take its place. Check that the CSP has built physical redundancy within its servers, within a data center and across separate data centers to protect against failures.

- Has the CSP built in redundancy at the Data level by replicating Data across geographically separate data centers to enable rapid recovery of Data?

- Does the CSP provide service resiliency e.g. using load balancing and constant recovery testing?

- Does the CSP limit the scope and impact of failure in one service area to that service area so that other service areas are not impacted?

- Look for CSPs that use simplified service components wherever possible so that there are fewer deployment and issue isolation complexities.

- Does the CSP provide real, rapid, and 24/7 on-call support? This should include access to engineers, product developers, program managers, product managers and senior leadership.

**Examples of regulations and guidelines that underpin this principle:**

- IRDA Guidelines, para 9.10
- IDRBT Cloud Security Framework p 19 & 20
- MAS Outsourcing Guidelines, Para 6.6
- MAS BCM Guidelines
- MAS TRM Guidelines
- MAS Outsourcing Questionnaire
- HKMA Outsourcing Guidelines, Para 2.7
- HKMA Technology Guidelines, Para 5.4
- HKMA BCP Guidelines
- APRA Outsourcing Standard, Para 23 and 41
- APRA BCM Standard
- APRA Data Risk Guide
Data Location
And Transparency

CSPs must disclose exactly where Data will be located. Government and BFSI companies should ensure that the Government policies, economic and legal conditions of the identified locations are safe and stable.

Government and BFSI Regulators typically require that Government and BFSI companies at all times know the exact location where a CSP will hold, store or process their Customer Data. A CSP’s data centers must be in safe, stable and secure places, where confidentiality and privacy obligations are observed, upheld and enforced by the local legal system.

In a number of countries, Government and BFSI companies will also need to know exactly where a CSP will hold, store or process their Personal Data. This is because Privacy Regulations in those countries typically do not allow Government and BFSI companies to transfer Personal Data overseas unless the Personal Data will be subject to a similar standard to the home jurisdiction’s Privacy Regulations. This may require additional contractual commitments or other safeguards to be put in place.

Government and BFSI Company Checklist:

• Has the CSP identified the exact locations where it will hold Data?
• Only use a CSP that will hold Data in safe and stable locations.
• Have you conducted a review to ensure that the Government policies, economic and legal conditions of the identified locations are safe and stable? Some Government and BFSI Regulators, such as the HKMA, for example, require a detailed assessment and legal opinion to be obtained. The CSP should be able to help with the risk assessment.
• Check whether there are any additional Privacy Regulation requirements in your country that will impact the transfer of Personal Data to any overseas locations. Make sure you put in place any necessary contractual or other commitments to ensure that these are complied with.

Examples of regulations and guidelines that underpin this principle:

- IRDA Guidelines, para 9.7
- IDRBT Cloud Security Framework, page 15, 26
- MAS Outsourcing Guidelines, Para 6.9
- MAS Outsourcing Questionnaire
- PDPA, Section 26
- HKMA Outsourcing Guidelines, Para 2.9
- HKMA Outsourcing Guidelines, Para 2.9 and PDPO, Section 33
Limits On Data Use

CSPs should not use Government and BFSI Companies’ Data for any purpose other than that which is necessary to provide the Cloud Service. The contract should prevent CSPs from using Government and BFSI Company Data for any secondary purpose at all times.

Government and BFSI Regulators generally require that Government and BFSI companies prohibit CSPs from using Customer Data for any unauthorized purposes (for example marketing and advertising). This helps to uphold the confidentiality of Customer Data and prevent it from being misused or disclosed (see Principle 4). If a CSP can use Customer Data for other purposes, it compromises the confidentiality of such data.

Privacy Regulations also typically require that Government and BFSI companies must not allow CSPs to use Personal Data for any purposes beyond the purpose for which the Personal Data was collected. This requirement protects individuals’ privacy so that their Personal Data is only used for purposes that the individuals would expect and have agreed to (i.e. the receipt of banking or other financial services).

**Government and BFSI Company Checklist:**

- Does the CSP commit that it will not use Data for any other purpose? Check, for example, that the CSP is not using the Data for the purposes of building analytics, data mining or advertising. You should contractually prohibit CSPs from using Data for any unauthorised purposes.
- Does the CSP commit to apply strict access controls so that access to Data is limited only to those within the CSP who require access to the Data to provide the Cloud Services? Check that the CSP reviews these access controls on a periodic basis.

**Examples of regulations and guidelines that underpin this principle:**

- IRDA Guidelines
- IT Act Rules 2011, Rule 4(iii), 5(3)(b), 5(5)
- IDRBT Cloud Security Framework, Page 25
- MAS Outsourcing Guidelines
- MAS Outsourcing Questionnaire
- PDPA, Section 18
Government and BFSI Company Customer Data must be segregated from other Data held by the CSPs. CSPs must be able to identify the Government and BFSI Companies’ Customer Data and at all times be able to distinguish it from other Data held by the CSP.

Government and BFSI Regulators require Government and BFSI companies to ensure their Customer Data is segregated from other Data, thereby ensuring that security and confidentiality of Customer Data is maintained (see Principle 4). This ensures that the integrity of Customer Data is preserved. Data segregation will also help make any termination easier to deal with since all Customer Data can be more easily returned and deleted (see Principle 10).

As noted above, Public Cloud and Community Cloud are multi-tenanted models. This means that multiple customers will be provisioned from a shared infrastructure. Multi-tenanted Cloud Services can still comply with Safe Cloud Principle 8, but only where the CSP has the ability to provide the services in a highly secure manner, so that data storage and processing for each tenant is separated.

**Government and BFSI Company Checklist:**

- Does the CSP ensure (and commit) that Customer Data will be segregated from other Data, especially from any Data of other customers of the CSP? Have they provided details as to how this is achieved?
- If you are looking at a multi-tenanted cloud solution, does the CSP segregate Data storage and processing for each customer so that one customer cannot access another’s Data held on the same infrastructure? A CSP who is not able to do so does not offer a Cloud Service that will meet these Principles.
- Does the CSP have technology specifically designed to safeguard Customer Data so that it cannot be accessed or compromised by co-tenants? Has the CSP provided you with a robust and clear explanation as to how it is able to ensure this?
Conditions On Subcontracting

CSPs may only use subcontractors if the subcontractors are subject to equivalent controls as the CSP.

Most CSPs will rely on the use of subcontractors to provide certain support services. This should not be a problem, but Government and BFSI Regulators require that subcontractors not be used unless the CSP ensures that the subcontractor will have equivalent protections and controls in place as the CSP. This principle ensures continued legal and regulatory compliance no matter who holds the Data or provides the services.

Privacy Regulations in certain countries also require that sharing Personal Data with subcontractors is subject to scrutiny to ensure that applicable commitments are met (notably in relation to security, transfers overseas and use of the Personal Data solely for the specified purposes and on behalf, ultimately, of the Government and BFSI Company).

✅ Government and BFSI Company Checklist:

- Has the CSP explained to you how and when it uses subcontractors? You should only use a CSP who will explain why the subcontractors will have access to the Data.

- Your CSP must be able to provide you with a list of the subcontractors that it uses and with any updates to this list over time.

- Does the CSP have in place controls to ensure that its subcontractors are subject to equivalent commitments? Security, confidentiality, limitation on use and transparency of exact location as well as the other Principles are all relevant here, and the CSP should be able to demonstrate that these principles are covered.
Examples of regulations and guidelines that underpin this principle:

- IT Act Rules 2011, rule 6(4) and 7
- IDRBT Cloud Security Framework
- MAS Outsourcing Guidelines, Para 6.4
- MAS Outsourcing Questionnaire
- PDPA, Section 17
- HKMA Outsourcing Guidelines, Para 2.6.
- PDPO, Schedule 1, Data Protection Principles, 4(2)
- APRA Outsourcing Standard, Para 25 and 26
- APRA Outsourcing Guide
- APP 6

Conditions On Termination

Government and BFSI companies must have appropriate exit provisions in the contract with the CSP. To the extent that the Government and BFSI Company requires that, on termination, the CSP must work with the Government and BFSI Company to return the Government and BFSI Companies’ Data to the Government and BFSI Company and then the CSP must permanently delete the Data from the CSP’s systems. Any Data that does not need to be returned to the Government and BFSI Company must be permanently deleted by the CSP.

Upon termination of a Cloud Service contract, Government and BFSI Regulators generally require that CSPs return, delete or destroy Customer Data (see Principle 4). If a CSP can continue to hold Customer Data after termination, that information’s confidentiality will be at risk.

In addition, Privacy Regulations in most countries require that Personal Data be deleted or destroyed when it is no longer required. This requirement protects individuals’ privacy so that their Personal Data will not be held for longer than is necessary by the CSP.

Government and BFSI Company Checklist:

- Does the CSP give a clear contractual commitment that it will work with you to return Data and then permanently delete it from its systems?
- Look for CSPs that use best practice procedures and a data wiping solution which are compliant with the National Institute of Standards and Technology’s Guidelines for Media Sanitization (set out in publication NIST 800-88).
- Check that the CSP uses a destruction process that destroys and renders the recovery of information
impossible for hard drives that cannot be wiped.

- ISO27001 accreditation will help in this respect since it requires secure disposal or re-use of equipment and disposal of media.

Examples of regulations and guidelines that underpin this principle:

- IRDA Guidelines para 9.9
- MAS Outsourcing Guidelines, Para 6.4
- MAS Outsourcing Questionnaire
- MAS TRM Guidelines
- PDPA, Section 25
- HKMA Outsourcing Guidelines, Para 2.5.4
- PDPO, Schedule 1, Data Protection Principles, 2(3)
- APRA Outsourcing Standard, Para 25
- APRA Outsourcing Guide, Para 15
- APP 11
**Advanced Encryption Standard:** A standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).

**APPs:** The Australian Privacy Principles. From 12 March 2014, the Australian Privacy Principles will apply to Government and BFSI Companies.

**APRA:** The Australian Prudential Regulation Authority. The Australian regulator for Government and BFSI Companies.

**APRA BCM Standard:** A prudential standard made by the APRA under the Australian Banking Act that all Government and BFSI companies must comply with, to deal with contingency issues. A legislative instrument.

**APRA Data Risk Guide:** Prudential Practice Guide CPG 235 – Managing Data Risk. APRA’s guide to assist Government and BFSI companies in appropriately managing their data risk.

**APRA Outsourcing Guide:** Prudential Practice Guide PPG 231 ― Outsourcing. APRA’s guide to assist Government and BFSI companies to comply with the APRA Outsourcing Standard and, more generally, to outline prudent practices in relation to managing outsourcing arrangements.

**APRA Outsourcing Standard:** A prudential standard made by the APRA under the Australian Banking Act that all Government and BFSI companies must comply with when outsourcing a material business activity. A legislative instrument.

**APRA Security Guide:** Prudential Practice Guide PPG 234 – Management of security risk in information and information technology. APRA’s guide to assist Government and BFSI companies in the management of security risk in information and information technology.

**Banking Ordinance:** The Hong Kong Banking Ordinance.

**Cloud Security Alliance (CSA) Cloud Control Matrix (CCM):** The CSA is a not-for-profit, member driven organization of leading industry practitioners focused on helping customers make the right decisions when moving into the cloud. The CSA published the CCM, which provides a detailed understanding of the security and privacy concepts and principles aligned to the CSA’s guidance.

**Cloud Services:** See “Overview of Cloud Services”. At its most basic, Cloud Services means on-demand network access to a shared pool of configurable computing resources.

**Community Cloud:** See Overview Section.

**CSP – Cloud Service Provider:** A third party that provides Cloud Services.
Customer Data: A subcategory of Data. Customer data, which may be defined differently from jurisdiction to jurisdiction, shall for the purposes of this document be generally taken to mean any data which relates to a customer of a Government and BFSI Company.

Data: When using Cloud Services, Government and BFSI companies may transfer various kinds of data to CSPs, for CSPs to help, store, destroy, manage and/or process. This data may include Government and BFSI Companies’ business confidential information, information about the Government and BFSI Companies’ clients, personal data relating to the Government and BFSI Companies’ clients and/or the Government and BFSI Companies’ employees. There are two key subcategories of Data: Customer Data and Personal Data.

Government and BFSI Regulator: A regulatory body with supervisory authority over Government and BFSI companies e.g. IRDA, MAS, HKMA and APRA.


IT Act: The Indian Information Technology Act 2000


FISMA: The US Federal Information Security Management Act requires US federal agencies to implement information security programmes. CSP’s may be granted authority to operate under FISMA by federal agencies. Operating under FISMA requires transparency and frequent security reporting to federal customers.

HIPAA: The US Health Government and BFSI Portability and Accountability Act. This US law applies to healthcare entities and governs the use, disclose and safeguarding of protected health information (PHI), and imposes requirements on covered entities to sign business associate agreements with their CSPs that have access to PHI.

HKMA: The Hong Kong Monetary Authority. The Hong Kong regulator for Government and BFSI Companies.

HKMA BCP Guidelines: Non-statutory guidelines published by the HKMA in its Supervisory Policy Manual, which the HKMA expects Government and BFSI companies to take into consideration in relation to business continuity planning.

HKMA Outsourcing Guidelines: Non-statutory guidelines published by the HKMA in its Supervisory Policy Manual, which the HKMA recommends that all Government and BFSI companies address when outsourcing their activities.

HKMA Technology Guidelines: Non-statutory guidelines published by the HKMA in its Supervisory Policy Manual setting out the general principles for technology risk management that all Government and BFSI companies are expect to consider in managing technology-related risks.

Hybrid Cloud: See Overview Section.
ISO27001: ISO 27001 is a system standard published by the International Organization for Standardization that formally mandates specific security requirements around management, systems and controls and incident management.

MAS: The Monetary Authority of Singapore. The Singaporean regulator for Government and BFSI Companies.

MAS Banking Secrecy Notice: MAS Notice 634 to Banks: Banking Secrecy – Conditions for Outsourcing.


MAS Outsourcing Questionnaire: MAS Technology Questionnaire on Outsourcing.

Personal Data: A subcategory of Data. Personal Data (or similar terms in laws or regulations) may be defined differently from jurisdiction to jurisdiction. For the purposes of this document, it broadly means any data that relates to an individual, including personally identifying information or information associated with or derived from an individual’s use of the Government and BFSI Companies’ financial services, or as a result of the relationship as a customer or employee of the Government and BFSI Company.


PDPO: The Hong Kong Personal Data (Privacy) Ordinance 1995 as amended by the Hong Kong Personal Data (Privacy) (Amendment) Ordinance 2012.

Privacy Regulations: Regulations that govern the Government and BFSI companies collection, use and disclosure of Personal Data e.g. the APPs, the PDPA and the PDPO.

Private Cloud: See Overview Section.

Public Cloud: See Overview Section.