Asia's Financial Services: Ready for the Cloud

A Report on FSI Regulations Impacting Cloud in Asia Pacific Markets

Asia's Financial Services: Ready for the Cloud

A Report on FSI Regulations Impacting Cloud in Asia Pacific Markets

Acknowledgments

This report is published by the Asia Cloud Computing Association, in partnership with Olswang Asia LLP.

The ACCA would like to acknowledge the following people for their contributions:

Stacy Baird, Chair, Data Governance Working Group, Asia Cloud Computing Association

Andrew Cooke, Microsoft

John Galligan, Microsoft

Michael Mudd, Asia Policy Partners LLC

Lim May-Ann, Executive Director of the Asia Cloud Computing Association

Ian Ferguson and Matthew Hunter, Olswang Asia LLP (www.olswang.com)

The ACCA would like to acknowledge the following organisations for their assistance with the jurisdiction annexes:

Armstrong Teasdale LLP, China (www.armstrongteasdale.com)

Trilegal, India (www.trilegal.com)

Bagus Enrico & Partners, Indonesia (www.bepartners.co.id)

Anderson Mori & Tomotsune, Japan (www.amt-law.com)

Zul Rafique & Partners, Malaysia (www.zulrafique.com.my)

Buddle Findlay, New Zealand (www.buddlefindlay.com)

SyCip Salazar Hernandez & Gatmaitan, the Philippines (www.syciplaw.com)

Eiger, Taiwan (www.eigerlaw.com)

Blumenthal Richter & Sumet, Thailand (www.brslawyers.com)

Frasers Law Company, Vietnam (www.frasersvn.com)

Table of contents

Executive Summary

A Report on FSI Regulations Impacting Cloud in Asia Pacific Markets

1. Cloud Services offer substantial benefits to FSIs. However, FSIs in APAC have generally been slow to adopt Cloud Services because of (at least in part) the perceived regulatory challenges.

2. There are regulatory requirements that must be addressed in order for an FSI to adopt Cloud Services but, when it comes to the scale of these challenges, there is often a misalignment between perception and reality. The analysis carried out in developing this report confirms that there are no "blanket bans" or similarly broad prohibitions or restrictions that should prevent FSIs in APAC from adopting (and, therefore, benefiting from) the use of Cloud Services. On the contrary, some jurisdictions are developing new regulations, which are not specific to Cloud Services but which clearly enable adoption of Cloud Services by FSIs, and several others are allowing cloud adoption under current regulations for outsourcing.

3. CSPs can contribute to the growth of Cloud Services in APAC by ensuring that they have a good understanding of the regulatory requirements. This report will equip CSPs with an understanding of the current regulatory landscape in APAC and their FSI customers' key regulatory challenges to the adoption of Cloud Services and it will help CSPs to develop and provide solutions to these challenges.

4. Regulators in APAC also have a key role to play in the growth of Cloud Services in APAC. This report identifies where and how Regulations currently allow FSIs to adopt Cloud Services and where there is room to improve the current regulatory landscape across APAC to promote the development of Cloud Services. It makes recommendations to Regulators to improve the current regulatory landscape. The top five recommendations are:

    - **Regulations should be technology neutral. There should not be separate regulations for the use of Cloud Services.**
    - **Regulations should set out a clear process that should be followed for the adoption of Cloud Services (as if it were any other form of outsourcing) and approval for the use of Cloud Services should not be required.**
    - **The transfer of Data to other jurisdictions should be permitted, subject to appropriate safeguards (e.g. security, business continuity, access and audit).**
    - **Regulations should only identify the key issues that should be addressed in outsourcing contracts that include Cloud Services. They should not be prescriptive of the terms of an outsourcing contract that includes Cloud Services.**
    - **The use of independent third party audits should be an acceptable alternative to audits carried out by FSIs and the Regulators.**

5. Finally, FSIs can maximise the benefits on offer from the use of Cloud Services by ensuring that they are familiar with the regulatory landscape, and able to assess the degree to which the CSP's offering fits into the regulatory landscape. This report will provide FSIs with a clear understanding of the regulatory landscape and what they can, and should, expect from their CSPs.

Part 1: Introduction

The primary purpose of this report

The primary purpose of this report is to equip CSPs with an understanding of the current regulatory landscape in APAC and their FSI customers' key regulatory challenges to adopting Cloud Services and to help CSPs to develop and provide solutions to these challenges. In particular, this report:

- provides CSPs with a database of issues and possible solutions to discuss with their FSI customers;
- provides CSPs with recommendations as to how to comply with the current regulatory landscape; and
- supports CSPs in their engagement with relevant governments and Regulators.

This report may also be used by Regulators and FSIs to understand the current regulatory landscape in APAC and the key opportunities and challenges to adopting Cloud Services.

FSIs have been slow to adopt Cloud Services. This report sees perceived regulatory challenges as one of the causes of this slow adoption. Sometimes there is a lack of Regulation. Sometimes it is not evident how the Regulations apply as they are unclear or appear to be too restrictive. If these challenges can be addressed FSIs will be encouraged to maximise the commercial benefits that can be obtained from Cloud Services. Therefore, this report also provides Regulators with recommendations as to how to improve the current landscape, based on best-practice international principles.

The best possible outcome following the publication of this report would be for all of the Regulators across APAC to work towards a common framework informed by the recommendations in this report. Regional forums such as Asia-Pacific Economic Cooperation (APEC) or the formation of the ASEAN Economic Community (AEC 2015) could encourage such an outcome. However, this is an ambitious, yet worthy, aspiration. Pending an APAC agreement on a common framework, it would help FSIs and CSPs if the Regulators individually implemented the recommendations in this report. If a common approach is taken in the financial services sector, this would also set a precedent for Regulators in other sectors and therefore could help businesses and organisations across all sectors to more easily adopt (and benefit from) Cloud Services.

This report can also be used by FSIs that are considering adopting Cloud Services. FSIs can use the same recommendations that this report provides for CSPs, in order to evaluate whether or not the solutions offered by CSPs meet the recommendations made in this report.

The structure of this report

Part 1 of this report is this introduction.

Part 2 of this report compares the laws and regulations that impact the adoption by FSIs of Cloud Services ("**Regulations**") in 14 jurisdictions across nine different topics. For each topic, there is: (a) an introduction to the topic; (b) an overview of the Regulations in the 14 jurisdictions; (c) a commentary on the general issues, trends and deviations for the topic; (d) a list of recommendations for CSPs, to help CSPs to comply with current Regulations; and (e) a list of

recommendations for Regulators to improve current Regulations. The nine topics were selected on the basis that they represent the most important regulatory issues that must be addressed for the adoption of Cloud Services.

Part 3 of this report lists all of the recommendations made by this report for CSPs.

Part 4 of this report lists all of the recommendations made by this report for Regulators.

Part 5 of this report includes annexes covering each of the 14 jurisdictions in more detail. Each annex contains: (a) an overview of the regulatory approach taken to Cloud Services in the jurisdiction; (b) a list of the Regulations in the jurisdiction; and (c) a summary of the key requirements in the Regulations.

Part 6 of this report is a glossary of defined terms that are used in this report.

Cloud Services are now widely adopted

FSIs (and customers in many other industries) are recognising the commercial benefits of, and will increasingly benefit from the use of, Cloud Services. The scalability, agility, security and cost effectiveness of Cloud Services offers significant commercial benefits to all customers, and that it is inevitable that Cloud Services will evolve into the mainstream of IT services provision, including for the financial services sector.

According to Forrester Research, the APAC Cloud Services market will grow from USD 6.9 billion in 2013 to USD 31.9 billion in 2020.[1] This push towards Cloud Services is not just happening in APAC; it is global.

IDC estimates that businesses will spend over USD 107 billion on Public Cloud Services in 2017.[2] This is a significant amount but it only represents a fraction of the estimated USD 2 trillion that companies will spend on information technology ("IT") generally. Gartner predicts that the majority of new IT spending by 2016 will be for Cloud Services platforms and applications, with nearly half of large enterprises deploying Hybrid Cloud Services by the end of 2017.[3]

The trend in favour of Cloud Services has been recognised by international standards organisations. The International Organization for Standardization (known as "ISO") published its first cloud-specific standard in August 2014: ISO/IEC 27018.[4] The standard focuses on the measures that a CSP should take when handling Personal Data. This new standard demonstrates the demand for Cloud Services but also recognises that there are risks to be addressed and provides a guideline for managing these. The standard provides a benchmark which helps CSPs to understand, and offer Cloud Services that comply with, the requirements set out in Privacy Regulations.

The standard can also be used by FSIs to identify any gap or deviation from what they should expect and require CSPs' Cloud Services to be compliant with Privacy Regulations.

---

1) Progress Exchange (Oct 2013). Asia Pacific: Entering the Market and Growing, https://www.progress.com/~/media/Progress/Documents/News%20and%20Events/Exchange2013/Track%208%20-%20Expand%20Market%20Grow%20PFuller%20v2.pdf

2) IDC (3 Sep 2013). IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation, http://www.idc.com/getdoc.jsp?containerId=prUS24298013

3) Gartner (24 Oct 2013). Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016, http://www.gartner.com/newsroom/id/2613015

4) ISO (29 Jul 2014). ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

Cloud Services will benefit FSIs but the risks need to be addressed

The cost advantages of Cloud Services are attractive to all customers, including FSIs. Since the global financial crisis revenues at FSIs have come under increased pressure and the cost of compliance with regulations has increased significantly. Cloud Services offer a way of improving cost-income ratios.

FSIs that use Cloud Services will also receive a competitive advantage over those in their industry that do not: CSPs can provide the most secure services, reliably and on a utility-based model that allows cost savings and offers agility that can flex to the customers' requirements. Adopters of Cloud Services can escape the encumbrances of their legacy IT systems and avoid regular and expensive upgrade work because of this new model of IT services.

FSIs have already started outsourcing the processing of Data that does not involve Customer Data or Personal Data but does require significant computing resources. This includes tasks such as running millions of analytics calculations with many different variables to assess the consequences of what may happen to their businesses and outlook in certain circumstances. These calculations can be done more quickly using Cloud Services. FSIs are also using Cloud Services when they need safe test and development environments in which they can mirror their own systems and then make changes or updates without the risk of affecting the rest of their operations. Sometimes referred to as "sand boxing", this method adds another layer of security to core banking systems by clear separation.

However, larger projects using Cloud Services for wholesale operations involving Customer Data and/or Personal Data can be more challenging (and have therefore happened less frequently). As mentioned above, this is in part because of the regulatory challenge. As this report will discuss, sometimes there is a lack of Regulation (e.g. see topics: (4) DATA USE LIMITATION; (5) SECURITY; and (6) DATA SEGREGATION) and sometimes it is not evident how the Regulations apply as they are unclear or appear to be too restrictive (e.g. see topics: (1) PROCESSES FOR ADOPTING CLOUD; (2) CONTRACTS FOR CLOUD SERVICES; (3) DATA LOCATION; and (8) AUDIT, REVIEW AND MONITORING).

It is also because FSIs are reluctant to trust a third party service provider with masses of Customer Data and critical processes.

Complex legacy systems at large FSIs can also make the transition to Cloud Services more difficult. These challenges may have slowed down the pace of adoption but this report submits that these challenges will not stop the eventual uptake of Cloud Services. In many cases, transitioning from legacy systems has become imperative given their age or complexity. Cloud Services offer a compelling technological and economic opportunity to encourage businesses to make this transition.

As mentioned above, the cost benefits will attract FSIs to Cloud Services. Their scalability, reliability and high security standards of Cloud Services will also attract FSIs. The security standards offered by CSPs can match and better those achievable by in-house IT systems at FSIs and CSPs are already working to demonstrate that this is the case by obtaining certifications and regulatory approval.

FSIs should also be aware of the use of Cloud Services by competitors. For example, there are an increasing number of competitors for FSIs in payment services. The likes of Alipay, Apple, Google, and PayPay are not traditional FSIs, but they offer alternative payment solutions, in

competition with FSIs. Twitter has entered the payments market, and Facebook provides payment functionality for apps and is looking into connecting payments functionality with its messenger service. These new market entrants use Cloud Services to gain a competitive advantage.

Cloud Services are important for the economy

McKinsey & Company projects that the total economic impact of Cloud Services could be USD 1.7 trillion to USD 6.2 trillion annually in 2025. Of this total, USD 1.2 trillion to USD 5.5 trillion could be in the form of additional surplus from use of Cloud Services, while USD 500 billion to USD 700 billion could come through productivity improvements for enterprise IT.[1] Gartner predicts that APAC Public Cloud Services spend could hit up to USD 7.4 billion by the end of 2015.[2]

Cloud computing is expected to create 14 million new jobs globally between 2011 and the end of 2015, of which about 10 million will be in APAC.[3]

Jurisdictions that implement Regulations at the right level (i.e. establish an appropriate balance between addressing the risks associated with Cloud Services whilst opening up the benefits of Cloud Services to businesses including FSIs) will enjoy greater economic benefits. The jurisdictions that do not achieve this balance will place their economies at a comparative disadvantage.

Additional information about the scope of this report

This report is not intended to be a comprehensive and detailed analysis of all the Regulations and their requirements, nor is it legal advice; rather it is intended to be a summary and to provide guidance. This report is not an exhaustive statement of all of the issues that may be relevant in all of the jurisdictions.

For the most part, the report will look at the Regulations that are relevant for banks and insurance companies. In some jurisdictions there are slightly different rules for certain types of FSIs. The jurisdiction annexes in Part 5 of this report highlight where this is the case but this report does not go into the detail. However, it is the view of the authors of this report that, generally, the Regulations, as they apply to the different categories of FSIs, are not fundamentally different. Therefore, the issues covered, the best practices and the solutions identified in this report should be broadly applicable across the financial services industry.

This report covers 14 jurisdictions in APAC: Australia, China, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, New Zealand, the Philippines, Singapore, Taiwan, Thailand and Vietnam. While the information is accurate to the best of the authors' knowledge at the date of publication (Feb 2015), updates to legislation may have since occurred.

---

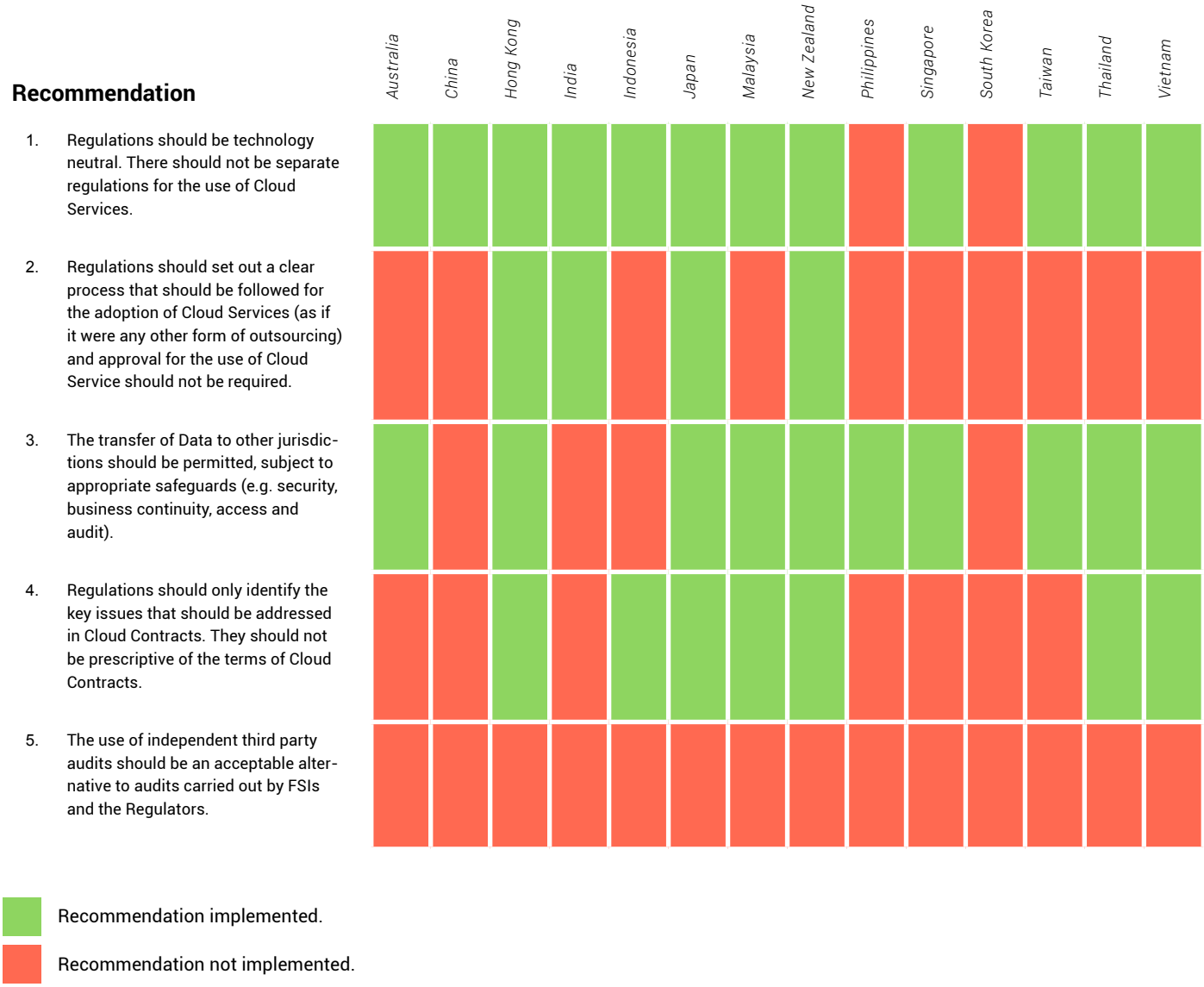
1) McKinsey Global Institute (May 2013). Disruptive technologies: Advances that will transform life, business, and the global economy, http://www.mckinsey.com/insights/business_technology/disruptive_technologies

2) ZDNet (January 2015). APAC public cloud spend to hit $7.4b in 2015: Gartner, http://www.zdnet.com/article/apac-public-cloud-spend-to-hit-7-4b-in-2015-gartner/

3) IDC (March 2012). Cloud Computing's Role in Job Creation, http://people.uwec.edu/HiltonTS/ITConf2012/NetApp2012Paper.pdf

Overall status of jurisdictions against the key recommendations

The table below shows whether or not, as of the date of publication of this report, each jurisdiction has implemented each of the top five recommendations this report makes to improve the current regulatory landscape:



The overview below shows the overall status of the jurisdictions against these key regulations:

Ranking	Jurisdictions
Five out of five	
Four out of five	Hong Kong, Japan and New Zealand
Three out of five	Malaysia, Thailand and Vietnam
Two out of five	Australia, India, Indonesia, Singapore and Taiwan
One out of five	China and the Philippines
Zero out of five	South Korea

Part 2: Comparison of Regulations in Nine Topic Areas

1. Processes for adopting Cloud

A. Introduction

The processes for adopting Cloud Services and the Regulations that apply differ from one jurisdiction to the next but there are many common themes. In some jurisdictions, the Regulations are not always clear. In most jurisdictions there are no Regulations that are specific to Cloud Services. Rather, the Regulations that are relevant to the use of Cloud Services apply more generally to outsourcing, which includes the use of Cloud Services.

As a minimum, all of the Regulators require FSIs to carry out a risk assessment and due diligence on the CSP and its Cloud Services. Some Regulators set out in more detail what this due diligence process must cover. This is typically in the context of Regulations or check lists for any IT outsourcing by an FSI. Many Regulators also require FSIs to notify the Regulator if they outsource services (this normally includes the use of Cloud Services) and sometimes there are prescribed processes and/or forms or documents that must be submitted. Finally, some Regulators require FSIs to obtain the Regulator's approval before FSIs engage a CSP for Cloud Services.

B. Overview

	Australia	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*	*New Zealand*	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
Is due diligence required?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are there specific Cloud Services regulations?	No	No	No	No	No	No	No	No	Yes	No	Yes	No	No	No
Is approval needed from Regulators?	No	No	No	No	Yes	No	2	No	Yes	No	No	3	1	No
Must the Regulators be notified?	1+2	Yes	No	2	Yes	No	Yes	No	Yes	1	Yes	3	1	No
Is there a prescribed document or questionnaire for FSIs to complete?	No	No	No	No	Yes	No	No	No	Yes	Yes	Yes	No	Yes	No

1 Yes – For "material" projects only.

2 Yes – If Data is transferred off-shore.

3 Yes – If Data is transferred offshore and for certain kinds of services.

C. Observations and issues

All of the Regulators require due diligence to be carried out but each jurisdiction has different requirements. It is no surprise that all of the Regulators across the 14 jurisdictions require FSIs to carry out a risk analysis and due diligence on the CSP and its Cloud Services (as they do for any outsourcing of regulated activities). In each jurisdiction, a risk analysis and due diligence should be completed prior to entering into the Cloud Contract. There are some differences between the Regulations because some of the Regulators are more prescriptive than others about what due diligence should be carried out. For example, the Regulators in Singapore and the Philippines have issued detailed questionnaires that must be completed by FSIs prior to entering into an outsourcing contract, which would include a Cloud Contract.

In Australia, Hong Kong, Singapore, South Korea and the Philippines, the Regulators set out certain requirements that should be verified by FSIs during the due diligence process (such as due diligence on the nature, scope and complexity of the outsourcing (including Cloud Services) to identify the key risks and risk mitigation strategies; an analysis of risk-return on the potential benefits of the proposed Cloud Services against the vulnerabilities that may arise and an analysis of the capabilities, reputation and financial standing of the CSP). However, many FSIs will already have their own detailed procurement processes which they will follow to ensure that they obtain the correct services and best commercial deal, and issues such as security and reliability are also addressed. A lot of FSIs (and companies outside the financial services sector) will do this even if there is no regulatory requirement to do so because it makes good business sense. The Financial Regulators are concerned about the higher risks involved in the financial services sector. This explains why Regulators have set out specific requirements in relation to the due diligence steps that must be taken by FSIs.

In some jurisdictions, FSIs must notify the Regulator about the use of Cloud Services. The requirement to notify the Regulator goes one step further. The Regulator is saying that, in addition to carrying out due diligence, FSIs must also notify the Regulator about the planned adoption of Cloud Services. Some Regulators require more information as part of this requirement than others. The Regulators in Singapore and in the Philippines require substantial additional information to be submitted including a completed questionnaire (in a prescribed form). Many Regulators (like those in Hong Kong and Korea) request to see copies of the Cloud Contract. The requirements differ across APAC and so the burden of compliance for international FSIs increases, since it is not possible to prepare one submission to notify all of the relevant Regulators.

In practice, a notification requirement sometimes becomes an approval requirement (although not expressly stated as an approval requirement). In some countries, there is no express requirement to obtain approval from the Regulator but there is a notification requirement (e.g. Australia, China, Singapore and South Korea). However, under this notification process the Regulator is able to ask the FSI questions. In practice, although this is a notification requirement and not an approval requirement, FSIs often wait until the Regulator confirms it has no further questions before proceeding with the adoption of the Cloud Services. Therefore, in practice, the notification requirement sometimes becomes an approval requirement. This circumstance would be improved if the Regulations set out clearly that there is no need to wait for a confirmation from the Regulator or includes a deadline for the Regulator to ask questions about the notification.

A limited number of Regulators require that the use of Cloud Services is approved by the Regulator. Some Regulators expressly require FSIs to obtain their prior approval. There is an express requirement in Indonesia and in the Philippines to obtain approval from Regulators. In

Thailand, only material transactions require the approval of the Regulator. However, the definition of "material" is not clear. This report does not agree with a requirement to obtain approval from a Regulator: it is not efficient and it is not always clear what is required or how approval relates to other regulatory requirements.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should assist FSIs through their due diligence process.** CSPs should help prepare documents and evidence to demonstrate that they have the requisite experience, competence, financial strength, resources and business reputation.
- **CSPs should demonstrate to FSIs that they can comply with the regulatory requirements.** CSPs should prepare documents and evidence to demonstrate how their Cloud Services can meet the requirements of the Regulations (e.g. security, limits on Data use, responsibility for subcontractors, Data location, rights to audit, review and monitor and exit provisions). The relevant jurisdiction annex in this report provides CSPs with a starting point to understand these requirements in more detail.
- **CSPs should assist FSIs to complete any questionnaires that the Regulators may require to be completed.** Generally, in these questionnaires, many of the questions that need to be answered will need input from the CSP, because the questions will require details about the Cloud Services (e.g. the security standards that are implemented by the CSP). The FSI customer is more likely to complete the process successfully with the CSP's help than without it.
- **CSPs should work with FSIs to address any deficiencies in the results of the due diligence prior to signing the Cloud Contract.** This includes deficiencies shown in the results of the due diligence against the legal, regulatory or business requirements.
- **CSPs should be transparent about any existing complaints and litigation.**

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulations should be clear and publicly available.**
- **Regulations should be technology neutral. Regulators should not set out separate regulations for the use of Cloud Services.** This will help to ensure they are fit for purpose and future-proofed in a fast-moving technology environment.
- **Regulations should set out a clear process that should be followed for the adoption of Cloud Services (as if it were any other form of outsourcing).** See the following recommendations for more specific details about what the process should be.
- **Approval for the use of Cloud Service should not be required.** Regulators should not require FSIs to obtain their approval before FSIs enter into a Cloud Contract. Regulators that require uses of Cloud Services to be approved may hinder business efficiency. As a minimum, Regulations should provide a deadline for approval and state that beyond this deadline, the project is deemed approved. However, importantly, an approval in itself may send the wrong message to FSIs. FSIs may believe that, with approval for its use of Cloud Services, the regulatory compliance has been completed. This is not the case. There are on-going obligations that are equally important for FSIs to comply with. A notification process can

instead give Regulators the opportunity to object to any proposals that are unsuitable (see the following recommendation).

- **If there is a notification requirement, Regulators should only require notification for a material use of Cloud Services. The notification requirement must include a well-defined materiality threshold.** As Cloud Services will become increasingly popular across businesses in the future, only a material use of Cloud Services should be subject to a requirement to notify the Regulator. If this regulatory approach is implemented, the term "material" should be clearly defined. This is for reasons of business efficiency as many business processes or data types will not be subject to the most rigorous oversight. Instead, Regulators could require FSIs to keep an internal record or database with regard to the Cloud Services that they use.
- **If there is a notification requirement, Regulators should publish what process should be followed, including the number of days' notice required to be provided by the FSI to the Regulator before the FSI will enter into the Cloud Contract.** The Regulator should also make clear in Regulations the maximum number of number of days the Regulator will take to respond to the notice. As a consequence, the FSI will know that after the notice period has expired, the FSI may enter into the Cloud Contract.
- **If there is a notification requirement, Regulators should set out clearly what information should be notified to the Regulator.** Regulators could do this by publishing questionnaires (see the following recommendation).
- **Regulators should publish a questionnaire that FSIs should complete before adopting Cloud Services.** The questionnaire should not be specific to Cloud Services but should apply to any form of outsourcing. The use of a questionnaire can help guide FSIs through the due diligence process and can form part of the FSI's internal record or database of the Cloud Services that they use.

2. Contracts for Cloud Services

A. Introduction

It is good business practice for an FSI to enter into a Cloud Contract[1] if it adopts Cloud Services. The Regulations in all 14 jurisdictions require FSIs to enter into Cloud Contracts. No Regulators currently set out a prescribed form of Cloud Contract but most of the Regulators require certain terms to be included in Cloud Contracts (but with differing degrees of detail).

B. Overview

	Australia	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*	*New Zealand*	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
Is a Cloud Contract required?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is there a prescribed form of Cloud Contract?	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Are there principles or prescribed terms that must be included?	Principles and prescribed terms	Principles and prescribed terms	Principles only	Principles and prescribed terms	Principles only	Principles only	Principles only	No	Principles and prescribed terms	Principles and prescribed terms	Principles and prescribed terms	Principles and prescribed terms	Principles only	Principles only

Either the Regulations do not require any principles or prescribed terms to be included in the Cloud Contract or the Regulations only require certain specific principles to be included in the Cloud Contract.

The Regulations require certain principles and certain prescribed terms to be included in the Cloud Contract.

The Regulations set out a prescribed form of Cloud Contract.

C. Observations and issues

In some jurisdictions, including Japan, India, Thailand and Vietnam, the terms that must be included in Cloud Contracts are only set out in a basic amount of detail. For example, in Japan the Regulations require that the issues of subcontracting, termination and audit are dealt with in the Cloud Contract. However, the Japan Regulations do not provide more detail than this. This means that the FSI may not be entirely sure what they should include in their Cloud Contracts and the CSP may not be willing to accept a term requested by the FSI on the basis that it is a regulatory requirement which is not clear. However, rather than adding a high degree of detail to Regulatory requirements (which may not be appropriate in all circumstances), Regulations should provide that these requirements may be taken on face value (i.e. the requirements to include limits on subcontracting, termination rights and/or audit rights) and where such provisions are included

1) "**Cloud Contract**" means the contract between the FSI and the CSP for the provision of Cloud Services, such as an outsourcing services agreement which includes the provision of Cloud Services.

in the Cloud Contract (albeit that the details of these provisions have been negotiated by the parties), then the requirements have been satisfied. This report recommends that this is the correct approach. Therefore, Regulators should set out the general requirements that should be addressed in the Cloud Contracts but should state that it is up to the parties to agree the detailed terms and conditions of the relevant provisions.

In other jurisdictions (e.g. Australia, China, India, the Philippines, Singapore, South Korea and Taiwan) the Regulations require certain principles and certain prescribed terms to be included in the Cloud Contract (but do not go so far as to prescribe a form of Cloud Contract). This report does not support this more detailed approach, since it can slow down the negotiation process and lead to disagreement between the parties because of differing understanding or interpretation of Regulations. However, even with the additional regulatory detail in these jurisdictions, there is not too much detail and there is still room for the parties to negotiate the contract terms and conditions to meet the real intention of the requirements. In addition, as mentioned above, the Regulators should make it clear that if these provisions are addressed in the Cloud Contract (and further details of these provisions have been negotiated by the parties), the requirements have been satisfied.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should agree to include in Cloud Contracts the terms that are required by the Regulations.** Where a contractual term is required to meet one of the requirements set out in the Regulations (e.g. security, limits on Data use, responsibility for subcontractors, data location, rights to audit, review and monitor and exit provisions), then CSPs should include these terms in their template Cloud Contracts or agree to include these terms if FSIs request them during the Cloud Contract negotiations. This requires CSPs to develop an appropriate understanding of Regulations, an understanding that will be enhanced by contract negotiations with FSIs.
- **CSPs should be willing to discuss the terms that are required by the Regulations with FSIs (and Regulators if necessary), where it is not clear exactly what the term must say in the Cloud Contracts (or where the parties cannot agree on what the term must say because of differing understanding or interpretation of Regulations).**

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulators should not specify a prescribed form of Cloud Contract.** There are numerous Cloud Services being adopted by FSI to meet a wide range of requirements. No single Cloud Contract form will necessarily address all of the variables associated with an FSI adopting Cloud Services now or in the future.
- **Regulators should state the specific principles that should be dealt with in Cloud Contracts (if any). Alternatively, Regulators could state that the parties are free to negotiate all of the terms in their Cloud Contracts, provided that there is a Cloud Contract and the other regulatory requirements have been addressed.** Examples of specific principles include security, limits on Data use, responsibility for subcontractors, data location, rights to audit, review and monitor, exit provisions). This report believes that both of these approaches are acceptable.

- **Regulators should not go into the detail of how all the terms should be addressed in the Cloud Contract.** Contracts are flexible tools and there are many ways to address each of these requirements in the Cloud Contract. Certain details do not need to be prescribed by the Regulators, including the effects on liability, the processes that the parties will follow, the consequences of exercising any rights and the financial consequences. The parties should be free to negotiate these details.

3. Data location

A. Introduction

For most Cloud Services, Data is transferred to a CSP that may host this Data using infrastructure that is located outside of the jurisdiction where the FSI is located. Therefore, Data may be transferred to other jurisdictions. All 14 jurisdictions have Regulations that deal specifically with transfers of Data to another jurisdiction.

Financial Regulators are concerned when Customer Data and an FSI's critical processes are transferred to other jurisdictions. Privacy Regulators are concerned when Personal Data is transferred to other jurisdictions. The reality is that Personal Data, Customer Data or "critical processes" will often be transferred to other jurisdictions when FSIs use Cloud Services and therefore restrictions on the ability of FSIs to do so will diminish many of the key the benefits an FSI can achieve using Cloud Services. FSIs should be permitted to use Cloud Services that are located in other jurisdictions.

Regulators are concerned about the transfer of Data to other jurisdictions for a number of reasons. Regulators want to ensure that the protection offered to the Data does not weaken when the Data leaves their jurisdiction. Will the Data be secure? Will the Data be kept confidential? Will the government in the other jurisdiction have access to the Data? Will the Data be maintained in a manner consistent with regulatory requirements? Is the other jurisdiction's regime a stable one, politically and economically? Are similar legal protections offered to the Data and can they be enforced? Will they be able to maintain regulatory oversight? Will they be able to access the Data and/or carry out audits? CSPs must help to address these concerns.

B. Overview

	Australia	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*
Can FSIs use Cloud Services that are located in other jurisdictions?	Yes	No	Yes	Yes	Yes	Yes	Yes
Key takeaway	Detailed requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction	All core systems including all Customer Data, must be maintained within China	Detailed requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction	If an FSI transfers its Data to another jurisdiction it must notify the Financial Regulator	Approval must be sought from the Financial Regulator but the requirements relating to a transfer of Data to another jurisdiction are unclear	FSIs must have in place appropriate safeguards	Detailed requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction
Which Regulations are relevant?	Privacy Regulations and Financial Regulations	Financial Regulations	Financial Regulations	Financial Regulations	Privacy Regulations and Financial Regulations	Privacy Regulations	Privacy Regulations and Financial Regulations
Must the exact location be disclosed to the FSI?	Yes	Yes	Yes	Yes	Yes	No	Yes

	New Zealand	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
Can FSIs use Cloud Services that are located in other jurisdictions?	Yes	Yes	Yes	No	Yes	Yes	Yes
Key takeaway	There are limited requirements relating to a transfer of Data to another jurisdiction	Limited requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction	Detailed requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction	FSIs are prohibited from transferring Data to another jurisdiction	Detailed requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction	Detailed requirements must be met but if they are satisfied the FSI can transfer Data to another jurisdiction	Certain kinds of Customer Data may not be transferred to another jurisdiction unless FSIs have obtained a permit from the Financial Regulator
Which Regulations are relevant?	Privacy Regulations	Privacy Regulations	Privacy Regulations and Financial Regulations	Privacy Regulations and Financial Regulations	Privacy Regulations and Financial Regulations	Financial Regulations	Privacy Regulations and Financial Regulations
Must the exact location be disclosed to the FSI?	No	No	Yes	Yes	Yes	No	Yes

FSIs are permitted to transfer Data to other jurisdictions with no obstacle at all or FSIs are only required to follow a simple procedure to allow the Data transfer and the procedure is formulaic.

FSIs are permitted to transfer Data to other jurisdictions but there are more serious regulatory challenges that must be dealt with. There is a procedure to follow and detailed requirements must be met. If the work is done to meet all of this, the outcome is likely to be positive i.e. the FSI can transfer the Data to other jurisdictions.

There is a procedure to follow and detailed requirements must be met. However, if the work is done to meet all of this, the outcome is still uncertain, either because the requirements are stricter, unclear or because the Regulator may still object.

FSIs are not permitted to transfer Data to other jurisdictions.

C. Observations and issues

Contrary to common perception, the use of Cloud Services provided from infrastructure that is located in other jurisdictions is rarely prohibited by Regulations in APAC. The Regulations (except for those in China and South Korea) do not prohibit the use of Cloud Services that are located in other jurisdictions. However, for nearly all of the jurisdictions, the international transfers are subject to certain requirements that, although sometimes very detailed, are (for the most part) clear to follow (e.g. Australia, Hong Kong, New Zealand, the Philippines, Singapore and Vietnam). The Regulator's requirements in other jurisdictions are not clear to follow (e.g. Indonesia which appears to have substantially curtailed the ability for FSIs to adopt Cloud Services).

However, even where there is no prohibition and the requirements are clear, there is a general perception held by FSIs and Regulators that Data should be held within their own jurisdictions. As Cloud Services become (and are recognised by FSIs and Regulators as) the norm, these perceptions should evolve and change. CSPs should help to change this perception and can do so by following the recommendations below. Some of the Regulations are clear and simple, for example, the FSI is commonly required to know exactly where their Data is held. This is a requirement of Regulations in Australia, Hong Kong and Singapore.

A requirement that is less clear (and common) is the requirement that the FSI must verify that the jurisdictions where there Data is held are stable jurisdictions (economically, legally and politically). This is a requirement in Australia, Hong Kong and Singapore. It is easier to name jurisdictions that might generally be considered not to be so stable and therefore not a suitable jurisdiction for Data to be held by CSPs, but it is more difficult to assess overall stability because many jurisdictions have varying degrees of economic, legal and political stability. There is no objective way to measure this. Regulators, FSIs and CSPs may also have differing views on "stability" which makes it hard to predict with certainty whether or not any particular jurisdiction is "compliant" with this requirement.

There is a similar lack of objective clarity in the Privacy Regulations. Privacy Regulations commonly require FSIs to ensure that the Data transferred is protected to a similar standard as the Privacy Regulations in the FSI's jurisdiction.[1] The problem is that it is not clear what this requirement means (more so, because the requirement often appears in Privacy Regulations which are new and untested or where further guidance is not available (e.g. Malaysia, the Philippines and Singapore)). Should the jurisdiction to which the Data is transferred have its own Privacy Regulations? How does the FSI know if the laws of that jurisdiction are sufficiently similar or of a similar standard? Is it sufficient if the FSI puts in place contractual protections which include similar protections (e.g. if the FSI is transferring Data to jurisdictions where there are no Privacy Regulations or where the Privacy Regulations are not considered "sufficiently similar")? How does the FSI know if the contractual protections are "sufficiently similar" to the Privacy Regulations in its own jurisdiction? The Singapore Privacy Regulator has provided some more detailed guidance on the subject, which is helpful because it explains that local laws, binding corporate rules and contractual obligations can be considered as part of this evaluation. However, there is no definitive answer in any of the jurisdictions.

1) This concept is expressed in different ways by different regulators, but this report has tried to capture the general approach.

Nearly all of the Regulators expect that the Data will be held securely when it is transferred to another jurisdiction. This is a repeat of the general requirements relating to security (see topic: (5) SECURITY). The Regulators commonly remind the FSI of the security requirement because they are concerned that, as a result of the transfer to another jurisdiction, the Data is at risk of being held less securely. However, there can never be a guarantee that Data, no matter where it is located (i.e. within or outside the jurisdiction), will always be protected. This is always a risk.

Financial Regulators sometimes require that they have rights of access, and the ability to audit, the Data that is transferred to another jurisdiction. The Financial Regulators in Australia, Hong Kong and Singapore include this as a specific requirement in their Regulations. Again, this is a repeat of the general requirements relating to access and audit (see topic: (8) AUDIT, REVIEW AND MONITORING). Some Regulators do not specifically state this as an issue where Data is transferred to another jurisdiction (e.g. New Zealand and Thailand) but these Regulators would still expect to retain a right to audit or access the Cloud Services even if Data has been transferred to another jurisdiction. However, as mentioned above in relation to security, Regulators should recognise that they will not always be guaranteed to be able to access Data, no matter where the Cloud Services are located (i.e. within or outside the jurisdiction). The benefits of transferring Data to other jurisdictions, including cost savings, efficiency savings and mitigation of the risk of holding all Data in the same place, outweigh this risk.

Some Regulators specifically state that if Data is transferred to another jurisdiction there is a risk that it might be accessed by regulators/authorities within those jurisdictions. For example, the Hong Kong and Singapore Financial Regulators state that the FSI should evaluate the extent and possibility of such access taking place. Again, it is not easy to assess this risk because there is not an objective standard. The reality is that regulators/authorities in other jurisdictions may make demands of a locally-situated FSI or a CSP. These demands can be reasonable, warranted and within the law in the particular jurisdiction, but might not always be.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should disclose exactly where Personal Data and Customer Data will be located.** Without this basic information it will be hard for an FSI to engage a CSP.
- **CSPs should hold Data in jurisdictions commonly recognised as "stable" jurisdictions.** CSPs should point to successful examples of where they already hold Data and where this has been done without disruption because of economic, legal or political issues in the relevant jurisdictions. CSPs should be confident that they do not have any reason to believe that these stable conditions might change in the relevant jurisdictions.
- **CSPs should hold Data in jurisdictions where confidentiality and privacy obligations are observed, upheld and enforced by the local legal system.**
- **CSPs should give contractual commitments that (and ensure that) FSIs will be able to monitor and review the Data.**
- **CSPs should allow Regulators access and audit rights to the Data that is transferred to another jurisdiction and ensure that these rights can be exercised.** See topic: (8) AUDIT, REVIEW AND MONITORING for more information about audit.

- **CSPs should have in place (and contractually commit to) strict security arrangements no matter where the Data is located.** The security measures should be certified, provide maximum protection and contractually commit to the same. See topic: (5) SECURITY for more information about security requirements.
- **CSPs should address the challenge of "perception" that international transfers of Data are not appropriate for FSIs.** CSPs that comply with the recommendations and solutions discussed in this report, no matter where the Data they hold is located, will help to change this perception. CSPs that adopt, and/or are certified according to, international standards (including the new ISO/IEC 27018) will also help to change this perception.

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulators should allow Data to be transferred to other jurisdictions.** This report does not agree with the position of the Regulators in China and South Korea to prohibit Data transfers. Many FSIs are international organisations that already share Data internationally (for good and proper reasons, including corporate governance, internal reporting, customer service and risk mitigation). The modern economy and globalisation mean that businesses need to take international approaches which include transferring Data to other jurisdictions. Many CSPs do not have DCs in every jurisdiction. It will be a challenge for an FSI to find a CSP with DCs in every jurisdiction where the FSI is present and, even if the FSI could, the cost of the CSP's (or CSPs') services will likely be more expensive and many benefits of Cloud Services, such as security and business continuity through data location, cost benefits of scale and consolidation of services will be lost.
- **Regulators should focus their efforts on trying to ensure that FSIs' Data continues to be appropriately protected regardless of the location of the Data.** A simple statement that the Regulations apply equally to Data in other jurisdictions as to Data held in the FSI's home jurisdiction could convey this to FSIs.
- **Regulators should introduce Regulations that protect Data that is hosted in DCs located in their jurisdictions, whether the Data comes from their jurisdictions or from overseas.** For example, Singapore's Privacy Regulations expressly apply to "data intermediaries" which would include a CSP hosting Data in Singapore for an FSI located in another jurisdiction.
- **Regulators should not list/name the jurisdiction to which they consider it is acceptable to transfer Data.** This is one of the approaches taken by Privacy Regulations in Europe. Creating and maintaining such a list is a time consuming exercise for Regulators which can be overly political and the approach does not recognise that the "stability" of any jurisdiction or their Regulations can rapidly change, with changes going undocumented for long periods of time between updates to the list. Having such a list does not eliminate the risks of transferring Data to other jurisdictions. A more prudent approach would be to set out appropriate requirements which enable the FSI to determine the appropriateness of a destination jurisdiction. Some FSIs may take more conservative approaches than others but, as long as it is clear that FSIs are responsible for making the right decisions, and that the Regulators will take action against those who take the wrong decisions, then the right balance has been struck. Overly prescriptive regulations will endanger the commercial advantages that CSPs may offer to FSIs.

4. Data use limitations

A. Introduction

In all 14 jurisdictions, the FSI must ensure that the CSP is not able to use the FSI's Data for any purpose other than that which is necessary to provide the Cloud Services.

B. Overview

	Australia	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*	*New Zealand*	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
Can CSPs use the Data for secondary purposes?	No	No	No	No	No	No	No	No	No	No	No	No	No	No

C. Observations and issues

All of the Regulators require that the FSI must prohibit the CSP from using Data for any unauthorised purposes (for example marketing and advertising). This helps to uphold the confidentiality of the Data and prevent it from being misused or disclosed. If a CSP can use the Data for other purposes, it compromises the confidentiality of the Data. Even where the Regulations do not expressly require this prohibition to be included in the Cloud Contract, in practice, in order to ensure that the CSP does not use the Data for secondary purposes, the Cloud Contract should include this prohibition.

Privacy Regulations also typically require that the FSI must not allow the CSP 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 (in most cases, the receipt of banking or other financial services). These limitations should not be cause for concern.

Data is increasingly being recognised as a more and more valuable asset and Regulators may need to consider, in the future, how to regulate in more detail other possible uses of Data. As Data analytics develop, FSIs and companies in other sectors will try to extend the scope of what they use Data for. A typical question is whether or not a company can anonymise Data and therefore analyse it without being in breach of the Regulations (or, if the CSP carries out the analysis on behalf of the FSI, without putting the FSI in breach of its obligations). However, even if the Data is anonymised, there is always a risk that the Data will later be de-anonymised. This risk increases as data analytics tools become more powerful. If this risk can be minimised then Regulators may allow this limitation on Data use to be relaxed. There is economic opportunity and social benefit in data analytics but there is a risk. Therefore, it is understandable why, for now, Regulators remain conservative in this area.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **The CSP should commit in the Cloud Contract that it will not use Data for any purpose other than to meet its obligations under the Cloud Contract.** The CSP should also confirm that it will not use the Data for the purposes of data analytics, data mining or advertising.
- **The CSP should commit to apply strict access controls.** Access to Data should be limited only to those within the CSP who require access to the Data to provide the Cloud Services.
- **The CSP should review these access controls on a periodic basis.**

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

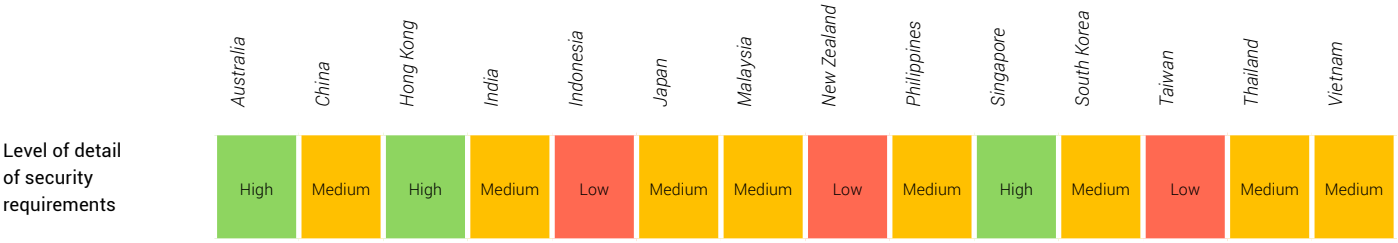
- **Commercial analysis of anonymised data should only be permitted if it is expressly authorised by the relevant FSI.**

5. Security

A. Introduction

As a minimum, the Regulations in all 14 jurisdictions require the FSI to ensure that the CSP maintains robust security measures and comprehensive security policies. Some Regulators go further and require the FSI to ensure that the CSP has implemented certain security measures. The level of detail of these security measures varies from jurisdiction to jurisdiction. Despite the differences, there is no doubt that security is one of the most critical requirements across the board. FSIs should not, and will not, use Cloud Services if they are not secure.

B. Overview



C. Observations and issues

All Regulators expect the FSI to place security requirements on the CSP but the level of detail of these security requirements varies from jurisdiction to jurisdiction (as shown in the overview above).

Low: The Regulations in Indonesia, New Zealand and Taiwan contain a low level of requirements i.e. there is not more than a general obligation in the Regulations to ensure that Data is kept secure by the CSP without any details on the specific security measures that should be put in place.

Medium: In China, India, Japan, Malaysia, Philippines, South Korea, Thailand and Vietnam the Regulations go into more detail than this. The Regulations in these jurisdictions specifically set out certain kinds of security measures that should be put in place e.g. encryption.

High: Singapore has the most detailed set of security requirements which the FSI must follow and ensure that the CSP complies with. The Singapore Regulations include more specific security measures that should be in place and contain more information about how and when specific security measures must be used.

Regulators (understandably) place a lot of emphasis on security. This protects Customers of FSIs, the FSI's reputation, maintains high levels of customer confidence and preserves the reputation of the jurisdiction's financial services sector. Security is also important to Regulators because it helps to combat the recent increase in frequency of cyber security threats which can have a material business impact and potentially impact on economies and national security.

In many of the jurisdictions, in addition to the Financial Regulations, maintaining confidentiality and security is also a legal requirement imposed by statute and/or by case law. For example, in Australia, Hong Kong, India, Malaysia, New Zealand and Singapore there are confidentiality requirements in case law. In addition, Privacy Regulations in most of the 14 jurisdictions require the FSI to maintain 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. However, these case law and Privacy Regulation requirements do not tend to include the same levels of detailed security requirements that are often seen in the Financial Regulations.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should assist FSIs to demonstrate that they meet the security requirements set out in the relevant Regulations with which FSIs must comply.**
- **CSPs should conduct penetration tests.** Penetration tests should enable continuous improvement of incident response procedures. CSPs should explain to FSIs the testing and frequency of testing. FSIs should not conduct penetration tests on the CSP. Instead penetration test results carried out by a third party should be made available to the FSI and the Regulator on request.
- **CSPs should be ISO/IEC 27001 certified.** Certification is an important benchmark that can be used to measure security standards. ISO/IEC 27001 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 FSIs, can be indicative of the application of industry best practice and should also be taken into consideration (e.g. if the CSP has been granted authority under FISMA[1] (the US Federal Information Security Management Act) or is HIPAA[2] compliant).
- **CSPs should consider complying with ISO/IEC 27018.** This is a new standard released in 2014. It is relevant for CSPs who process Personal Data. It builds upon the security standards in ISO/IEC 27002. There is no certification programme yet available for ISO/IEC 27018 and that may remain the case. However CSPs should consider ISO/IEC 27018 and consider if they are willing to commit to comply with its terms e.g. in the Cloud Contract.
- **CSPs should consider the security and privacy criteria in the Cloud Control Matrix[3] (CCM).** The CCM was developed by the Cloud Security Alliance[4] to help potential customers of Cloud Services evaluate different CSPs.

1) The US Federal Information Security Management Act requires US federal agencies to implement information security programmes. CSPs may be granted authority to operation under FISMA by federal agencies. Operating under FISMA requires transparency and frequent security reporting to federal customers.

2) HIPAA: The US Health Insurance 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.

3) https://cloudsecurityalliance.org/research/ccm/

4) The Cloud Security Alliance (CSA) is a not-for-profit, member driven organisation of leading industry practitioners focused on helping customers make the right decisions when moving into the cloud.

- **CSPs should consider what additional commitments they can provide beyond certification.** CSPs should consider providing commitments in Cloud Contracts that cover 24-hour monitoring of physical hardware, secure networks, encryption of Data in transit and encryption of the hardware being used to host the Data.
- **CSPs should consider using Advanced Encryption Standard[1].**

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulators should approve the use of international standards.** There is a trend for Regulators to set out in detail the security requirements in their Regulations. Regulators should consider, instead of "re-inventing the wheel", endorsing international standards. If Regulators do not believe that these standards are adequate, Regulators should identify the areas that are insufficient and layer these on top of the international standards. International standards could be updated to reflect the insufficiencies. Regulators are not always the experts when it comes to security, so it would be sensible to leverage the work already done by security experts. As international standards are also updated (as technologies advance) the Regulators will only need to check that this updating is being done by the relevant internationals standards organisations.
- **Regulators should keep in mind that security cannot be guaranteed and should not use this as a reason to restrict the use of Cloud Services.** It is not possible for CSPs to guarantee the security of Data (nor is it possible for FSIs to guarantee the security of Data, even if they do not use Cloud Services). There will be security breaches. However, this does not mean that Cloud Services should not be used. In fact, the market leading CSPs are able to offer some of the best security controls available (possibly even better that the FSIs are able to implement themselves in their own IT infrastructure). Regulators should be concerned about the security levels at CSPs but this concern should not develop into a restriction on using Cloud Services. This benefits of Cloud Services should outweigh the apparent risk, especially if you consider that the risk is possibly no bigger (possibly even smaller) than the technology risk that already exists in-house at FSIs.

1) The Advanced Encryption Standard is the standard for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).

6. Data segregation

A. Introduction

In many of the jurisdictions, the FSI is required to ensure that its Data is segregated from other Data held by the CSP. This means that the CSP must be able to identify the FSI's Data and at all times be able to distinguish it from other Data held by the CSP.

B. Overview

	Australia	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*	*New Zealand*	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
Is there a data segregation requirement?	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Does Data have to be physically segregated?	No	No	No	No	No	No	No	No	No	No	No	No	No	No

C. Observations and issues

Many Regulators require the FSI to ensure its Data is segregated from other Data held by the CSP. This requirement helps to ensure that security and confidentiality of Data is maintained. This requirement also helps to ensure that the integrity of Data is preserved. Data segregation will also help make termination of the Cloud Contract easier to deal with since all the FSI's Data can be more easily returned and deleted.

This requirement is most important for Public Cloud Services because they are multi-tenanted models. This means that multiple customers will be serviced from shared infrastructure. Multi-tenanted Cloud Services can comply with this requirement 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. This is often referred to as logical separation (rather than physical separation). Whilst CSPs may also be able to provide additional options to FSIs for physical separation (e.g. Community Cloud Services or Hybrid Cloud Services), physical separation is incongruous with the economic benefits of Public Cloud Services and therefore physical separation should not be required by the Regulators. No Regulator currently requires physical separation.

A numbers of jurisdictions do not have a requirement that the Data is segregated. This report recommends that all Regulations include this requirement. However, the requirement should not say that the Data should be physically isolated or segregated. If the requirements stated this, then FSIs would be unable to use Public Cloud Services even where otherwise appropriate. Currently, this is not the case in any of the jurisdictions.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should ensure (and commit) that one customer's Data will be physically or logically segregated from the Data of other customers.** CSPs should provide detailed information as to how this is achieved.
- **Where a CSP logically segregates Data, the CSPs must logically segregate Data storage and processing for each customer.** One customer of the CSP should not be able to access another customer's Data held on the same infrastructure.
- **CSPs should have technology specifically designed to safeguard Data so that it cannot be accessed or compromised by other customers of the CSPs.** CSPs should provide robust safeguards and a clear explanation as to how they are able to ensure this.

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

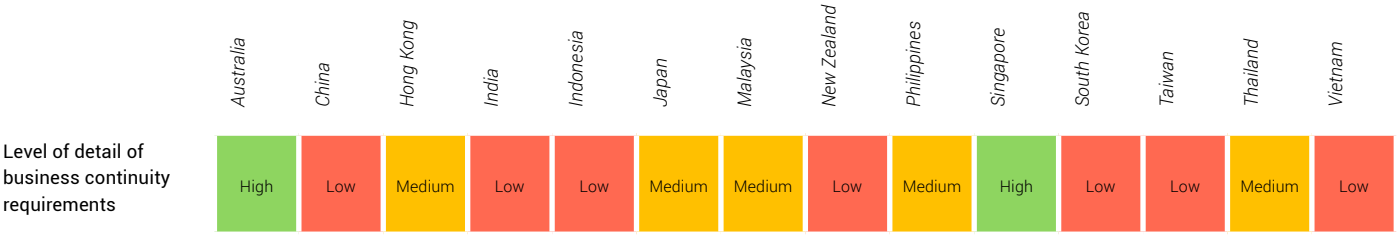
- **Regulators should require that one FSI's Data will be segregated from the Data of other FSI customers.**
- **Regulators should acknowledge (and explain in their guidance to FSIs) that segregation can be done by logical separation and does not require physical separation.**

7. Business continuity

A. Introduction

Cloud Services must be reliable. As a minimum, all of the Regulators require that the FSI has effective business continuity plans 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 minimised through effective and appropriate planning and procedures and a high degree of system resilience.

B. Overview



C. Observations and issues

All Regulators require the FSI to impose business continuity requirements on the CSP but the level of detail of these business continuity measures varies from jurisdiction to jurisdiction. Depending on the jurisdiction, FSIs are expected to meet the requirements set out in one of the following broad categories.

Low: The Regulations in China, India, Indonesia, New Zealand, South Korea, Taiwan and Vietnam contain a low level of requirements i.e. there is no more than a general obligation to ensure that the Cloud Services are reliable with limited details on the specific business continuity requirements that should be put in place.

Medium: In Hong Kong, Japan, Malaysia, the Philippines and Thailand, the Regulations go into more detail than those Regulators in the Low category and require FSIs to ensure that certain standards of business continuity should be met, that there should be restoration targets for the CSPs, that the plans should be tested and/or that interruptions must be reported.

High: Singapore has the most detailed set of business continuity requirements which the FSI must follow and ensure that the CSP complies with. The Singapore Regulations go into detail about what the targets should be and also include reporting requirements if the target is breached.

This principle is important to Regulators because service disruption can have significant impact on the wider community. Regulators recognise that service disruptions can happen but require that the risk of them arising and their effect are minimised by having in place appropriate business continuity plans and procedures. The FSI must ensure these plans and procedures are in place and are regularly tested and updated, to protect against service disruption.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should be able to demonstrate that consistently high levels of service availability have been achieved.** CSPs should demonstrate this according to their track records on service continuity (e.g. over the past five years).
- **CSPs should 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). CSPs should provide FSIs with financial compensation for failure to meet this service availability, to back up this commitment (e.g. service credits).
- **CSPs should apply an "active-active" configuration (where appropriate).** An "active-active" configuration means that if a failure occurs in one server or DC, another server or DC can take its place. An active-active configuration may not always be appropriate (depending on the kind of Cloud Service being provided); the more critical the Cloud Services are to an FSI, the more likely that an "active-active" configuration is required.
- **CSPs should build physical redundancy within their servers, within a DC and across separate DCs to protect against failures.**
- **CSPs should build in redundancy at the Data level by replicating Data across geographically separate DCs to enable rapid recovery of Data.**
- **CSPs should provide service resiliency e.g. using load balancing and constant recovery testing.**
- **CSPs should limit the scope and impact of failure in one service area to that service area so that other service areas are not impacted.**
- **CSPs should use simplified service components wherever possible so that there are fewer deployment and issue isolation complexities.**
- **CSPs should provide real-time, rapid and 24/7 on-call support.** This should include access to engineers, product developers, program managers, product managers and senior leadership.

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulators should include, as a minimum, a requirement that there must be business continuity arrangements in place between the FSI and the CSP.** Regulators may also set out more detailed business continuity requirements to the extent that the detail serves to describe a baseline, or they may leave it to the parties to decide and agree this detail.

8. Audit, review and monitoring

A. Introduction

Compliance does not end when the outsourcing contract that includes Cloud Services is signed. This is a clear requirement of the Regulators. The FSI is required to obtain regular reporting and information from the CSP to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the outsourcing contract that includes Cloud Services. In many jurisdictions the requirements go further and require the FSI and the CSP to meet regularly to review the reports and performance levels. Many Regulations also require audit rights, either for the FSI (sometimes recognising that this audit can be carried out by a third party), the Regulator or both. Allowing for audit rights often cause difficulties for the CSP.

B. Overview

Do the regulations require...	*Australia*	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*	*New Zealand*	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
...that the FSI has rights to review and monitor the CSP?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
...that the Regulator has a right to audit the CSP?	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
...that the FSI has a right to audit the CSP?	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	No	Yes

C. Observations and issues

Regulators recognise that the FSI may need to outsource certain services but they make it clear that the FSI cannot outsource their primary responsibility for risk and compliance. This is why Regulators require the FSI to continue to review compliance by the CSP. The FSI must continue to be vigilant in compliance throughout the Cloud Contract lifecycle. The requirements to continue to review and monitor the performance of the CSP appear in all of the jurisdictions.

Most Regulators require that the CSP provides the Regulator with rights to carry out an audit or an inspection of the CSP. All of the jurisdictions (except for Japan and New Zealand) require that the Regulators have a right to audit the CSP. The purpose of this requirement is to enable the Regulator to confirm itself (should it wish to do so) that the CSP is complying with the contractual, legal and business requirements.

Regulators commonly require that the FSI has a right to audit the CSP. This allows the FSI to confirm itself (should it wish to do so) that the CSP is in compliance, rather than relying on the information provided by the CSP.

CSPs are reluctant to allow unlimited audit rights (and rightly so). For valid reasons, including protection of the Data of their other customers and minimising disruption to their business operations, CSPs would prefer to limit the audit rights to those which are necessary to assess compliance in respect of the customer in question. None of the jurisdictions explain what the scope of the audit rights is, how often they should be able to be exercised, who should pay for the audit, how long the audit can last for, how many people can participate in the audit, what obligations are placed on the auditors during the audit and what happens to the audit results. These questions remain unanswered in all 14 jurisdictions. It seems that, in principle, audit rights are desired but, in practice, the detail has not been fully set out. This can cause difficulty when these rights are being negotiated. First, because the FSI is not sure exactly what the scope of the audit rights should be and second, because the CSP is reluctant to grant wide ranging audit rights. CSPs may view a Regulator audit as better than an FSI audit, because this will limit the number of audits that it has to offer. However, questions still remain about the scope of the audit rights and whether or not the Regulators are best placed to conduct the audit.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should regularly (e.g. annually) provide FSIs 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 FSIs with copies of reports of penetration testing that the CSP has carried out or arranged to be carried out by independent third parties.
- **CSPs should give FSIs a full overview of the testing, review and audits that they conduct, or have third parties conduct, on a regular basis.** CSPs should be prepared to have their processes verified.
- **CSPs should be transparent and provide FSIs with real-time and continuous information.** This should include information about the current availability of the services, history of availability status, details about service disruptions and outages and scheduled maintenance times.
- **CSPs should provide FSIs with access to an account manager in order to assist in the management of performance and problems.**
- **CSPs should include in Cloud Contracts provisions for escalation of issues that arise.**
- **CSPs should agree in Cloud Contracts to allow audits by the FSI and/or the applicable Regulators where required to do so by the Regulations.** However, CSPs will have valid reasons to be reluctant to grant such audit rights. Therefore, CSPs should, as a minimum, work with FSIs (and applicable Regulators if necessary) to provide alternative means for the FSIs (and applicable Regulators) to obtain the comfort that they require e.g. by agreeing in Cloud Contracts to adequate reporting requirements, third party audits and/or certification or even limited audit rights. As an alternative to granting audit rights to FSIs and/or applicable Regulators, CSPs could arrange for independent certification and third party audits to be carried out. This alternative may not meet the current regulatory landscape but this report recommends (below) that Regulators recognise this alternative approach.

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulators should permit on-going independent certification as an adequate alternative to audit rights for Regulators and FSIs.** Regulators should recognise that a CSP that has obtained and maintains independent certification (e.g. security certification), has demonstrated the necessary continuing compliance. So, if a CSP has, and maintains, its ISO 27001 certification, Regulators should recognise that the CSP meets a standard that is generally considered the most appropriate certification for the CSP given the high benchmark that the CSP must meet to achieve and maintain that certification.
- **Regulators should permit independent third party audit results as an adequate alternative to audit rights for Regulators and FSIs.** Instead of requiring that the FSI and the Regulator have a right to audit the CSP, the Regulator could instead accept the results of an independent third party audit of the CSP. This should be more acceptable to CPSs, because it would limit the number of audits that would need to take place. For example, the CSP might only need to allow one independent third party to audit its Cloud Services annually and the results of this audit could then be shared with FSIs and Regulators. The Regulators would need to agree on the scope of the audit, the scope of access that the Regulator and the FSI should have to the third party auditor (e.g. to ask questions) and how the results could be used, but an independent third party audit process could be a much more efficient way to verify compliance by CSPs. A periodic independent third party audit programme could cover a greater scope than the scope that could be covered by FSIs and Regulators (if they carried out their own audits of the CSP). This report recommends that the independent third party audit of the CSP should be carried out annually. The audit should cover, as a minimum, security measures, business continuity measures, data segregation measures, checks that Data is not being used for other purposes, checks that Data has been deleted where an FSI has requested that the Data should be deleted, checks that the same measures are in place in other jurisdictions, if the Data has been transferred to other jurisdictions.

9. Exit

A. Introduction

Most Regulators require the FSI to have exit provisions in Cloud Contracts. Generally, the FSI must, on termination, be able to require the CSP to work with the FSI to return Data to the FSI. In all cases the FSI must also require the CSP to delete the Data from the CSP's systems.

B. Overview

	Australia	*China*	*Hong Kong*	*India*	*Indonesia*	*Japan*	*Malaysia*	*New Zealand*	*Philippines*	*Singapore*	*South Korea*	*Taiwan*	*Thailand*	*Vietnam*
Does the Cloud Contract have to include termination rights?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Does the CSP have to return Data on termination?	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes	Yes	No	Yes	No
Does the CSP have to delete Data on termination?	Yes	Yes	Yes	No	No	Yes	No	No	Yes	Yes	No	No	Yes	No

No, but confidentiality must be protected.

C. Observations and issues

Some Regulators require that the FSI have certain termination rights in their Cloud Contracts. In South Korea, the Regulations require that the FSI must be able to terminate the Cloud Contract if the Regulations have been breached. In Singapore the Regulations require that the FSI must be able to terminate the Cloud Contract for default, including change of ownership, insolvency events, a breach of security or confidentiality, or a "demonstrable deterioration in the ability of the service provider to perform the service". It can be difficult for the CSP to agree to all of these termination rights without further negotiation; the CSP and the FSI will have to negotiate the consequences of all of these termination rights.

Upon termination of a Cloud Contract, Regulators generally require that the FSI ensures that the CSP deletes the Data. This principle helps maintain and safeguard the confidentiality of Data. If a CSP can continue to hold Data after termination, the Data's confidentiality will be at risk. In addition, Privacy Regulations in most countries require that Personal Data is deleted 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. A number of jurisdictions do not have clear requirements that the Data must be deleted by the CSP upon termination of the Cloud Contract, including India, Indonesia and Taiwan. Whilst CSPs are required to delete Data, it is not always

technically possible to wipe all Data and, therefore, as long as the recovery of Data from the hard drives is not possible, the obligation to delete has been satisfied. No Regulators expressly recognise this fact.

Regulations in some jurisdictions require that the FSI has a right to obtain a copy of the Data upon termination of the Cloud Contract. This is the case in Australia, China, Hong Kong, Japan, Malaysia, the Philippines, Singapore, South Korea and Thailand. This right is useful for the FSI because it can make the process of bringing the Cloud Services back in-house or transferring the Cloud Services to another CSP more efficient. This is not yet a requirement in India, Indonesia or Taiwan.

None of the Regulations recognise that a right to obtain a copy of the Data coupled with an obligation on the CSP to delete all Data provides the best safety net to safeguard the FSI and its Data. As long as the FSI has these rights, the FSI should be adequately safeguarded, even if there are limited termination rights in the Cloud Contract.

D. Recommendations and solutions for CSPs to comply with the current regulatory landscape

- **CSPs should give a clear contractual commitment that it will work with the FSI to return Data and then permanently delete it from its systems upon the FSI's request.** The return of the Data does not mean that the CSP has to be actively involved in the work to return the Data. Depending on the type of Cloud Services, it might be enough that the CSP provides access to the FSI (for a certain period of time e.g. 90 days) in order for the FSI to obtain a copy of the Data. Once done, it is important that the CSP then deletes all of the Data from its systems: the FSI should have the Data that it needs and the CSP should no longer have this Data.
- **CSPs should use the best practice procedures for Data wiping.** CSPs should consider procedures that are compliant with the National Institute of Standards and Technology's Guidelines for Media Sanitization (set out in publication NIST 800-88).
- **CSPs should delete Data by using a process that renders the recovery of information impossible for hard drives that cannot be wiped.**
- **CSPs should consider ISO 27001 accreditation because it requires secure disposal or re-use of equipment and disposal of media.**

E. Recommendations and solutions for Regulators to improve the current regulatory landscape

- **Regulators should not set out what termination rights must be included in the Cloud Contract.** Where Regulators do list certain kinds of termination rights that must be included, Regulators should let all the parties freely negotiate the commercial consequences of exercising those rights.

- **Regulators should require CSPs to include in their Cloud Contracts a right for the FSI to obtain a copy of its Data from the CSP (at any point in the term of the Cloud Contract) and an obligation on the CSP to delete all Data upon termination of the Cloud Contract.** This will safeguard the FSI and their Data, no matter what the termination rights are. Regulators should also provide that the FSI is free to exercise these two rights at its own discretion. This is important because the FSI may require the CSP to continue to store its Data for a longer period following the termination of the Cloud Contract, e.g. in order to comply with data retention requirements or business continuity requirements during a service transition period.

Part 3: List of Recommendations for CSPs

CSPs should:

1. assist FSIs through their due diligence process;
2. demonstrate to FSIs that they can comply with the regulatory requirements;
3. assist FSIs to complete any questionnaires that the Regulators may require to be completed;
4. work with FSIs to address any deficiencies in the results of the due diligence prior to signing the Cloud Contract;
5. be transparent about any existing complaints and litigation;
6. agree to include in Cloud Contracts the terms that are required by the Regulations;
7. be willing to discuss the terms that are required by the Regulations with FSIs (and Regulators if necessary), where it is not clear exactly what the term must say in the Cloud Contracts (or where the parties cannot agree on what the term must say because of differing understanding or interpretation of Regulations);
8. disclose exactly where Personal Data and Customer Data will be located;
9. hold Data in jurisdictions commonly recognised as "stable" jurisdictions;
10. hold Data in jurisdictions where confidentiality and privacy obligations are observed, upheld and enforced by the local legal system;
11. give contractual commitments that (and ensure that) FSIs will be able to monitor and review the Data;
12. allow Regulators access and audit rights to the Data that is transferred to another jurisdiction and ensure that these rights can be exercised;
13. have in place (and contractually commit to) strict security arrangements no matter where the Data is located;
14. address the challenge of "perception" that international transfers of Data are not appropriate for FSIs;
15. commit in the Cloud Contract that it will not use Data for any purpose other than to meet its obligations under the Cloud Contract;
16. commit to apply strict access controls;
17. review these access controls on a periodic basis;
18. assist FSIs to demonstrate that they meet the security requirements set out in the relevant Regulations with which FSIs must comply;
19. conduct penetration tests;
20. be ISO/IEC 27001 certified;
21. consider complying with ISO/IEC 27018;
22. consider the security and privacy criteria in the CSA's Cloud Control Matrix (CCM);
23. consider what additional commitments they can provide beyond certification;
24. consider using Advanced Encryption Standard;

25. ensure (and commit) that one customer's Data will be physically or logically segregated from the Data of other customers;
26. Where a CSP logically segregates Data, the CSPs must logically segregate Data storage and processing for each customer;
27. have technology specifically designed to safeguard Data so that it cannot be accessed or compromised by other customers of the CSPs;
28. be able to demonstrate that consistently high levels of service availability have been achieved;
29. give a tangible commitment to high availability of service;
30. apply an "active-active" configuration (where appropriate);
31. build physical redundancy within their servers, within a DC and across separate DCs to protect against failures;
32. build in redundancy at the Data level by replicating Data across geographically separate DCs to enable rapid recovery of Data;
33. provide service resiliency e.g. using load balancing and constant recovery testing;
34. limit the scope and impact of failure in one service area to that service area so that other service areas are not impacted;
35. use simplified service components wherever possible so that there are fewer deployment and issue isolation complexities;
36. provide real-time, rapid and 24/7 on-call support;
37. regularly (e.g. annually) provide FSIs with copies of independent third party audit results that the CSP has obtained, e.g. SSAE 16 SOC1 (Type II) reports;
38. give FSIs a full overview of the testing, review and audits that they conduct, or have third parties conduct, on a regular basis;
39. be transparent and provide FSIs with real-time and continuous information;
40. provide FSIs with access to an account manager in order to assist in the management of performance and problems;
41. include in Cloud Contracts provisions for escalation of issues that arise;
42. agree in Cloud Contracts to allow audits by the FSI and/or the applicable Regulators where required to do so by the Regulations;
43. give a clear contractual commitment that it will work with the FSI to return Data and then permanently delete it from its systems upon the FSI's request;
44. use the best practice procedures for Data wiping;
45. delete Data by using a process that renders the recovery of information impossible for hard drives that cannot be wiped; and
46. consider ISO 27001 accreditation because it requires secure disposal or re-use of equipment and disposal of media.

Part 4: List of Recommendations for Regulators

Regulators should:

1. ensure that Regulations are clear and publicly available;
2. ensure that Regulations are technology neutral;
3. set out a clear process that should be followed for the adoption of Cloud Services (as if it were any other form of outsourcing);
4. not require approval for the use of Cloud Service;
5. if there is a notification requirement, only require notification for a material use of Cloud Services. The notification requirement must include a well-defined materiality threshold;
6. if there is a notification requirement, publish what process should be followed, including the number of days' notice required to be provided by the FSI to the Regulator before the FSI will enter into the Cloud Contract;
7. if there is a notification requirement, set out clearly what information should be notified to the Regulator;
8. publish a questionnaire that FSIs should complete before adopting Cloud Services;
9. not specify a prescribed form of Cloud Contract;
10. state the specific principles that should be dealt with in Cloud Contracts (if any). Alternatively, state that the parties are free to negotiate all of the terms in their Cloud Contracts, provided that there is a Cloud Contract and the other regulatory requirements have been addressed;
11. not go into the detail of how all the terms should be addressed in the Cloud Contract;
12. allow Data to be transferred to other jurisdictions;
13. focus their efforts on trying to ensure that FSIs' Data continues to be appropriately protected regardless of the location of the Data;
14. introduce Regulations that protect Data that is hosted in DCs located in their jurisdictions, whether the Data comes from their jurisdictions or from overseas;
15. not list/name the jurisdiction to which they consider it is acceptable to transfer Data;
16. only permit commercial analysis of anonymised data if it has been expressly authorised by the relevant FSI;
17. approve the use of international standards;
18. keep in mind that security cannot be guaranteed and not use this as a reason to restrict the use of Cloud Services;
19. require that one FSI's Data will be segregated from the Data of other FSI customers;
20. acknowledge (and explain in their guidance to FSIs) that segregation can be done by logical separation and does not require physical separation;
21. include, as a minimum, a requirement that there must be business continuity arrangements in place between the FSI and the CSP;

22. permit on-going independent certification as an adequate alternative to audit rights for Regulators and FSIs;
23. permit independent third party audit results as an adequate alternative to audit rights for Regulators and FSIs;
24. not set out what termination rights must be included in the Cloud Contract; and
25. require CSPs to include in their Cloud Contracts a right for the FSI to obtain a copy of its Data from the CSP (at any point in the term of the Cloud Contract) and an obligation on the CSP to delete all Data upon termination of the Cloud Contract.

Part 5: Jurisdiction Annexes

Note: There are hyperlinks where the Regulations are available online and, where available, these are links to English translations that have been prepared by Regulators. However, the translations may not always reflect the latest version of the Regulations since translations may not be regularly updated. Therefore, they should be used only for reference and should not be relied upon.

1. Australia

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Australian Prudential Regulatory Authority (www.apra.gov.au) (**"APRA"**). The Office of the Australian Information Commissioner (www.oaic.gov.au) (**"OAIC"**).
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No. However, FSIs (other than regulated superannuation entities) must notify APRA after entering into agreements to outsource material business activities and consult with APRA before outsourcing a material business activity to a CSP outside of Australia. For all other outsourcing activities, no APRA notification or consultation is needed.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No. There are no specific forms or questionnaires that an FSI must complete when considering Cloud Services.
Are there specific contractual requirements that must be adopted?	Yes. APRA does stipulate some specific points that FSIs must ensure are incorporated in their Cloud Contracts. These are set out in Section 25 of the APRA Outsourcing Guide.

Other information/developments	The 13 Australian Privacy Principles ("APPs") which are contained in schedule 1 of the Privacy Act 1998 ("Privacy Act") came into force on 12 March 2014. The APPs regulate the handling of Personal Data by Australian government agencies and private sector organisations. The Financial System Inquiry's Final Report (published on 7 December 2014) identified the great potential of Cloud Services to improve the efficiency, productivity and innovation within the financial services sector. Australian Cyber Security Centre ("ACSC") was launched in November 2014, which released cloud computing security documents in December 2014.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
APRA Prudential Standard Outsourcing	APRA Outsourcing Standard	APRA	CPS 231
APRA Prudential Practice Guide: Outsourcing	APRA Outsourcing Guide	APRA	PPG 231
APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology	APRA Security Guide	APRA	CPG 234
APRA Prudential Standard: Business Continuity Management	APRA BCM Standard	APRA	CPS 232
Privacy Act 1988	Privacy Act	OAIC	No. 119, 1988

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a third party, it has undertaken certain steps by way of due diligence.	APRA Outsourcing Guide, Section 25 APRA Outsourcing Standard, Section 23
Review, monitoring and control	FSIs must have established procedures for monitoring performance under the Cloud Contract on a continuing basis. FSIs must have a Board-approved policy in relation to the outsourcing, which must "set out its approach to outsourcing of material business activities, including a detailed framework for managing all such outsourcing arrangements".	APRA Outsourcing Standard, Sections 19 and 23(e)
Audit	The FSI must ensure that the CSP: (a) provides APRA with information/documents; (b) allows APRA and the FSI to conduct on-site visits; and (c) conducts an audit when requested to do so by APRA or the FSI.	APRA Outsourcing Standard, Section 19
Confidentiality and security	FSIs must ensure that CSPs implement an appropriate IT security risk management framework with the aim of maintaining confidentiality, integrity and availability and adopt a robust physical security in accordance with the APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology. Cryptographic techniques would normally be used to control access to sensitive data/information, both in storage and in transit.	APRA Security Guide, Sections 13, 71, 50, 51 and 56 Privacy Act, APP 11
Resilience and business continuity	CSPs must develop and maintain a business continuity plan that documents procedures and information which enable the FSIs to manage business disruptions. CSPs must review the business continuity plan annually and periodically arrange for its review by the internal audit function or an external expert. FSIs must notify APRA in the event of certain disruptions.	APRA BCM Standard

Data location	There is no prohibition on transferring Personal Data outside of Australia provided that an entity takes reasonable steps to ensure that the overseas recipient does not breach the APPs. FSIs must consult with APRA if they are planning on using Cloud Services provided from another jurisdiction. The due diligence process must include an examination of the relevant foreign legislation and regulations by a suitably qualified expert to ensure that contractual provisions are recognised by the foreign jurisdiction and are able to be enforced in the chosen jurisdiction.	Privacy Act 1988, APP 8 APRA Outsourcing Guide, Section 26
Data use	CSPs must not use or disclose FSIs' Data for any other purposes other than to provide the Cloud Services.	APRA Outsourcing Guide, Section 26 (b). Privacy Act 1988, APP 6
Data segregation	CSPs must be subject to appropriate Data controls including Data segregation.	APRA Security Guide, Section 48
Subcontracting	Cloud Contracts must include specific rules, or limitations to, subcontracting arrangements (for example, notification to the FSI prior to entering into a subcontracting arrangement). CSPs may only use subcontractors if the subcontractors are subject to equivalent standard in respect of security and confidentiality of Data, offshoring compliance with relevant legislation and regulations, and APRA's access to Data held by the CSP.	APRA Outsourcing Standard, Section 26 (l) APRA Outsourcing Guide, Sections 9, 10 and 13
Termination	The Cloud Contract must set out possible reasons for termination and procedures to be followed in the event of termination, including notice periods, the rights and responsibilities of the respective parties and transition arrangements. Transition arrangements would normally address access to, and ownership of, documents, records, software and hardware.	APRA Outsourcing Standard, Section 26 (i) APRA Outsourcing Guide, Section 15 APRA Security Guide, Section 55

2. China[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	China Banking Regulatory Commission (www.cbrc.gov.cn/english/index.html, 中国银行业监督管理委员会) (**"CBRC"**). China Insurance Regulatory Commission (www.circ.gov.cn/tabid/2746/Default.aspx, 中国保险监督管理委员会) (**"CIRC"**). China Securities Regulatory Commission (www.csrc.gov.cn/pub/csrc_en/, 中国证券监督管理委员会) (**"CSRC"**). Ministry of Industry and Information Technology (www.miit.gov.cn, 中华人民共和国工业和信息化部) (**"MIIT"**)[2] .
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No. There is no published law that requires a regulatory approval. However, BFIs and IFIs (as defined in the footnote below) are subject to reporting obligations. BFIs: BFIs that intend to conduct "major outsourcing"[4] must report the details to the CBRC.

1) Prepared with assistance from Armstrong Teasdale LLP (www.armstrongteasdale.com).

2) Chinese law classifies FSIs into three categories: (i) Banking Financial Institutions ("BFI"); (ii) Insurance Financial Institutions ("IFI"); and (iii) Security Financial Institutions ("SFI"). The three categories of FSIs are governed by three authorities, i.e. CBRC, CIRC and CSRC (respectively). As of the date of this report, CBRC and CIRC have published a number of rules to regulate the outsourcing of IT development and maintenance (see Section B). CSRC and MIIT have been moving slowly but are expected to introduce new rules in the near future.

3) BFIs include all banks, commercial banks, financial assets management companies (i.e. State-owned companies established to acquire and dispose of the bad debts incurred by Chinese State-owned banks), savings banks, rural credit associations, trust companies, group finance companies and financial leasing companies in China.

4) There is no clear definition of "major outsourcing".

In addition, certain types of outsourcing[1] must be reported to the CBRC at least 20 working days before the execution of the Cloud Contract.

It is very likely that Cloud Services will be caught. The 2013 BFI IT Outsourcing Guidelines do not give a deadline for the CBRC to complete its review and these guidelines are also silent on whether the BFI can still go ahead and execute the Cloud Contract whilst CBRC is reviewing the Cloud Contract. In practice, it is advisable for the BFI to first contact the CBRC before it will move forward and execute the Cloud Contract.

If the CBRC believes that the proposed Cloud Services will pose significant risks to the BFI's systems, the CBRC has the authority to suspend the execution of the Cloud Contract and demand the BFI and the CSP to rectify to the satisfaction of the CBRC.

BFIs are not allowed to outsource IT services overseas unless the Financial Regulator in that overseas country has signed a memorandum of understanding with CBRC in this regard.[2] However, BFIs are only allowed to outsource IT services overseas for "non-core" business. BFIs' Customer Data is seen by Chinese government as "critical to State security" and therefore must be maintained within Mainland China.

IFIs: IFIs[3] must report to the CIRC for any outsourcing of DC, IT infrastructure and disaster recovery. However, CIRC has not provided any detailed rules on the process of such reporting.

---

1) Seven types of outsourcing that will require prior reporting to the CBRC:
(1) Outsourcing of all IT work;
(2) Outsourcing of all DC or disaster recovery centre;
(3) Outsourcing involving the transfer, analysis and processing of BFI's Customer Data, transaction data and any other sensitive information;
(4) Outsourcing of BFI's system, where the service is conducted on a Not-on-site basis and the Customer Data is stored collectively;
(5) Outsourcing to an affiliate;
(6) Outsourcing overseas;
(7) Any other outsourcing that is considered as material by CBRC.

2) As at the date of publication, CBRC has signed MOUs on exchanges of regulatory information with more than 27 countries and territories (www.cbrc.gov.cn/chinese/home/docView/2008040913EA2DA45289CDC5FFD4A6F1E3FAAD00.html). The details of such MOUs do not seem to have been made available to the public. It is advisable for BFIs to consult with CBRC on a face-to-face basis before they will conduct off-shore sourcing.

3) IFIs are all insurance companies and insurance assets management companies in China.

Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	Yes for BFIs. No for IFIs and SFIs. BFIs: There are detailed procedures and requirements for any major outsourcing by BFIs. CBRC has not formally introduced any format questionnaire for BFIs to fill out.[1] BFIs are required to conduct extensive due diligence[2] before signing up for any IT outsourcing project and evaluate whether the proposed service complies with applicable regulatory requirements in relation to issues such as data security, confidentiality and disaster recovery. For "not-on-site and collective outsourcing"[3], the BFI must also prepare a risk assessment report about the CSP.
	The BFI then will need to submit the due diligence report, the risk assessment report (for Not-on-site and collective outsourcing) and the Cloud Contract to the CBRC for review. Although there is no express requirement for the BFI to wait for CBRC approval, in practice the CBRC has the authority to suspend the execution of the Cloud Contract if it believes that the proposed arrangement will pose significant risks to the BFI's system.
Are there specific contractual requirements that must be adopted?	Yes for BFIs and IFIs. No for SFIs. BFIs: The 2013 BFI IT Outsourcing Guidelines (Articles 34 to 37) requires that a BFI must sign both an Outsourcing Agreement and a Service Level Agreement with a CSP. These must contain certain specific contractual arrangements. More details are set out in Section C. The 2009 BFI IT Risk Management Guidelines provided some factors that BFIs must consider in negotiation with CSPs (Article 58).

1) CBRC published a draft BFI Information Technology Risk Regulation Questionnaire earlier for public comments. This questionnaire include questions with respect to IT outsourcing but is not specifically designed for outsourcing reporting and CBRC has not made it clear when this questionnaire will become effective.

2) The due diligence must cover: (1) the technical expertise, service experience, personnel skills, business goodwill and regulatory compliance of the service provider; (2) the integrity, level and means of internal control and management of the service provider; and (3) the business continuity of the service provider, particularly the operation history, competitiveness, business prospective, financial capacity and profitability of the service provider.

3) The 2014 BFI Not-on-site and Collective IT Outsourcing Guidelines defines this as outsourcing where "the key infrastructure and information system is not located in premises owned or operated by the BFI and the system resources is leased or purchased by the BFI". Please note that these guidelines only apply to outsourcing providers that maintain and operate services for more than three BFIs at the same time.

There are more restrictive requirements if the outsourcing will involve not-on-site and collective IT outsourcing (see Article 6 of 2014 BFI Not-on-site and Collective IT Outsourcing Guidelines).
IFIs: The Cloud Contract must contain specific clauses with respect to the scope of service, safety and confidentiality, IP, continuity of services, dispute resolutions, modification or termination of agreement, exit provisions and liability for breach of contract.

Other information/developments

In December 2013, CBRC held a conference in Beijing to celebrate the establishment of the Association of BFI IT Outsourcing Service Providers. 27 service providers joined the association and signed the Articles of Association. According to CBRC, this association will serve as a "platform for self-regulation" for the service providers. Going forward, the association will conduct industrial evaluation of the service levels of the service providers.

In 2012, MIIT approved a plan to draft three national industrial standards for IT outsourcing services. These will cover data protection, system delivery and maintenance as well as emergency response. To date, none of the standards has been published.

In 2014, CBRC published a number of official opinions with respect to safety and control of Information Technology in the financial services sector. These opinions seem to suggest that CBRC encourages BFIs to choose services providers who are willing to share core IP and know-how with the local BFIs and should avoid relying too much on external service providers. Many believe that these opinions also show that the Chinese Regulators prefer the adoption of open source technology in China's financial services sector.

The Chinese Cloud Services market has a high market entry barrier for Non-Chinese CSPs. Setting up of foreign invested companies is subject to approval by MIIT. Chinese IT and foreign investment law also prohibits foreign invested companies to directly engage in the provision of IDC, ISP, ICP and international VPN services, which are essential to Cloud Services. Foreign CSPs have to structure wisely in order to be able to provide Cloud Services legally in China.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
2006 Management Measure on Electronic Banking (Chapter 5)	E-bank Management Measures	CBRC	银监会令[2006]年第5号
2009 Guidelines on the Risk Management of Information Technology of BFI	2009 BFI IT Risk Management Guidelines	CBRC	银监发[2009]19号
2013 Guidelines on the Risk Management of Information Technology Outsourcing by BFIs	2013 BFI IT Outsourcing Guidelines	CBRC	银监发[2013]5号
2014 Guidelines on the Enhancement of Risk Management of Not-on-site and Collective IT Outsourcing by BFIs	2014 BFI Not-on-site and Collective IT Outsourcing Guidelines	CBRC	银监办发[2014]187号
2011 Trial Guidelines on the Security and Management of Information System of Insurance Companies	2011 Insurance IT Security and Management Trial Guidelines	CIRC	保监发[2011]68号
2008 Guidelines on Management of Disaster Recovery of Insurance Information	2008 Insurance Disaster Recovery Guidelines	CIRC	保监发[2008]20号
2012 Trial Guidelines on the Risk Management of Information Technology of BFIs in Guangdong	Guangdong BFI IT Risk Management Trial Guidelines	Guangdong CBRC	粤银监发[2012]42号
2013 Shenzhen Guidelines on the Management of Information Technology Outsourcing by FIs (Non-compulsory)	Shenzhen FI IT Outsourcing Guidelines	Shenzhen Market Supervision Administration ("MSA")	SZDB/78-2013
2013 Regulations on Telecommunications and Internet User Personal Information Protections	Internet Personal Data Protection Regulations	MIIT	工业和信息化部令第24号

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	BFIs: BFIs must carry out due diligence on the CSP to ensure that the CSP and its Cloud Services meet legal, regulatory, contractual and business requirements. If the outsourced services are considered as "Not-on-site and collective outsourcing", the BFI must additionally carry out an additional risk assessment (as mentioned in Section A). IFIs: IFIs must establish a system to evaluate and examine CSPs.	2013 BFI IT Outsourcing Guidelines, Article 28 2014 BFI Not-on-site and Collective IT Outsourcing Guidelines, Article 3 2011 Insurance IT Security and Management Trial Guidelines, Article 52
Review, monitoring and control	BFIs: BFIs must be able to monitor and control the CSP by requiring regular reports from the CSP. The Cloud Contract must provide a mechanism for remedial actions for any issues that emerge. Data must be preserved for at least one year after the termination of the service; the BFI must conduct an appraisal of the service level of the CSP upon the termination. The result of such appraisal will be taken as a reference when considering whether the CSP should be allowed to continue to provide services. IFIs: IFIs must regularly evaluate, examine and assess whether the CSP has been meeting the requirement for outsourcing.	2013 BFI IT Outsourcing Guidelines, Article 41 - 47 2014 BFI Not-on-site and Collective IT Outsourcing Guidelines, Article 7 2011 Insurance IT Security and Management Trial Guidelines, Article 54
Audit	BFIs: CSPs engaged by BFIs will be subject to audits by CBRC. The BFIs must conduct at least one comprehensive audit on the CSPs every two years. Key Outsourcing Service Providers[1] must hire a third-party auditing firm to assess the risks of its business annually and submit an annual report to CBRC. IFIs: CSPs engaged by IFIs will be subject to audits by CBRC.	2013 BFI IT Outsourcing Guidelines, Article 35(4), Art 75 2014 BFI Not-on-site and Collective IT Outsourcing Guidelines, Article 4 2011 Insurance IT Security and Management Trial Guidelines, Article 55

1) A CSP will be considered as a Key Service Provider under CBRC rules if it: (i) provides any of the following outsourcing services on a not-on-site basis: trading system and collective storage of Customer Data; or analyse and process Customer Data, transaction data or any other sensitive information of BFIs; or provide DC, disaster recovery centre and infrastructure to BFIs; and (ii) provides such outsourcing services to more than one-third of BFIs in the relevant market; or provides such outsourcing services to more than three BFIs which carry out inter-provincial business; or provide such outsourcing services to more than ten BFIs.

Confidentiality and security	BFIs: BFIs must adopt a "sound and robust" technology risk management framework and consider carefully the use of IT outsourcing services under the CBRC's IT related guidelines. CSPs must maintain robust security measures and comprehensive security policies. CSPs must use encryption technology to protect and secure the BFI's Data at all times. BFIs must set out detailed confidentiality terms in the Cloud Contract. Personnel of CSPs may only access the Data of BFIs on a "need to know" and "minimum authorization" basis. CSPs must ensure that all of its staff, agents, management, directors and other relevant personnel comply with the same confidentiality obligations. IFIs: CSPs must ensure safety of information.	2009 BFI IT Risk Management Guidelines, Article 60 2013 BFI IT Outsourcing Guidelines, Article 36 2011 Insurance IT Security and Management Trial Guidelines, Article 57
Resilience and business continuity	BFIs: CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives. CSPs must regularly test and update procedures and systems in place to meet those objectives. The risks of downtime must be minimised through good planning and a high degree of system resilience. IFIs: CSPs must maintain continuity of service and ensure that the change of its personnel will not impact such continuity.	2013 BFI IT Outsourcing Guidelines, Article 48 to 51 2011 Insurance IT Security and Management Trial Guidelines, Article 57
Data location	BFIs: BFIs must ensure that all its "core system", including all Customer Data, account information and product information are maintained within the border of Mainland China. IFIs: The 2011 Insurance IT Security and Management Trial Guidelines specifically required that all core servers, core DCs and disaster recovery must be located within the border of Mainland China. The CIRC rule does not give a definition on "core sever". This seems to suggest that severs and DCs other than those specified can be located outside of Mainland China. Other National Laws: There is no unified Personal Data protection law in China to date but ISPs and organizations processing personal information online (likely to cover both FSIs and CSPs) are required to comply with the 2013 Regulations on Telecommunications and Internet User Personal Information Protections. These Regulations include some very basic security requirements.	2009 BFI IT Risk Management Guidelines, Article 7(11) 2011 Insurance IT Security and Management Trial Guidelines, Article 23 2013 Regulations on Telecommunications and Internet User Personal Information Protections 2010 State Secrets Law

	Further, China's 2010 State Secrets Law prohibits any person to "mail or ship State secrets abroad; carry or transport State secrets abroad without approval" or "transmit State secrets, through wire or wireless communication on the Internet or other public network without employing data protection measures." This could be a challenge to CSPs because the definition of "State secret" under Chinese law is very broad and can be subject to the discretion of the Regulators.	
Data use	CSPs must not use BFI's Data for any purpose other than that which is necessary to provide the services.	2014 BFI Not-on-site and Collective IT Outsourcing Guidelines, Article 6(5)
Data segregation	Data of BFIs must be segregated from other data held by the CSPs. CSPs must be able to identify the BFI's Data and at all times be able to distinguish it from other data held by the CSP.	2009 BFI IT Risk Management Guidelines, Article 60(1) 2014 BFI Not-on-site and Collective IT Outsourcing Guidelines, Article 6(4)
Subcontracting	BFIs: BFIs must strictly control any subcontracting of the CSPs. The Cloud Contract must expressly provide that CSPs shall not subcontract any service without agreement by the BFI. Subcontracting is only allowed if: (1) the services subcontracted are not the core service; (2) the CSP shall remain responsible for the subcontractor, and the subcontractor must be subject to equivalent controls as the CSP; and (3) the CSP shall continually monitor the subcontractor and apply for the BFI's approval for any replacement of subcontractor. IFIs: IFIs must strictly control any subcontracting of the CSPs. IFIs must take measures to ensure that the subcontracting will not in any way lower the quality and safety of the outsourced services.	2009 BFI IT Risk Management Guidelines, Article 60(5) 2013 BFI IT Outsourcing Guidelines, Article 37 2011 Insurance IT Security and Management Trial Guidelines, Article 56
Termination	BFIs must have appropriate exit provisions in the Cloud Contract. Upon termination, the CSP must cooperate with the BFI to return the BFI's Data to the BFI. The CSP must permanently delete the Data from the CSP's systems. For any material breach by the CSP, the BFI must be able to unilaterally terminate the Cloud Contract and report such breach to CBRC. Such information will be shared with all BFIs. CBRC can ban the breaching CSP for at least two years if the breach is deemed by CBRC to be serious.	2009 BFI IT Risk Management Guidelines, Article 60(6) 2013 BFI IT Outsourcing Guidelines, Article 35(5), 49 – 51, 88

3. Hong Kong

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Hong Kong Monetary Authority (www.hkma.gov.hk, 香港金融管理局)) ("HKMA") regulates banks ("**Banks**"). The Insurance Authority in Hong Kong (www.oci.gov.hk, 保險業監理處) ("IA") regulates insurance companies ("**Insurers**"). The Office of the Privacy Commissioner for Personal Data (www.pcpd.org.hk, 香港個人資料私隱專員公署) ("**PCPD**").
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No. There are no specific forms or questionnaires that an FSI must complete when considering Cloud Services.
Are there specific contractual requirements that must be adopted?	Yes for Banks. These are not set out by HKMA in a comprehensive list but the Guidelines on Outsourcing and Technology Risk Principles do contain certain provisions which HKMA states should be set out in the Bank's Cloud Contract. No for Insurers. The IA does not specifically mandate contractual requirements that must be agreed by Insurers with their CSPs. However, the Guidance Note on Outsourcing does contain a long list of matters that it says that Insurers should "consider" when negotiating the contract.
Other information/developments	In December 2014, the PCPD published a Guidance Note for cross-border data transfers. Although the restriction on cross-border data transfers in Section 33 of of the PDPO is not yet in force, this Guidance Note is to help data users to prepare for the implementation of Section 33.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
HKMA's Guidelines on Outsourcing	HKMA Outsourcing Guidelines	HKMA	SA-2
HKMA's General Principles for Technology Risk Management	HKMA Technology Guidelines	HKMA	TM-G-1
Guidance Note on Outsourcing	IA Outsourcing Guidance	IA	GN 14
Personal Data (Privacy) Ordinance	PDPO	PDPC	(81 of 1995 as amended)

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	Before selecting a CSP, Banks must perform appropriate due diligence. Banks must ensure that the proposed outsourcing arrangement has been subject to a comprehensive risk assessment (in respect of operational, legal and reputation risks) and that all the risks identified have been adequately addressed before launch. Before selecting a CSP, Insurers must perform due diligence on the CSP (including considering factors such as aggregate exposure to the CSP, possible conflict of interests that may arise and price vis a vis the benefit gained in assessing and selecting a CSP). Insurers must ensure that the proposed outsourcing arrangement has been subject to a comprehensive risk assessment (in respect of financial, operational, legal and reputation risks and any potential losses to its Customers in the event of a failure by the CSP to perform) and that all the risks identified have been adequately addressed before launch.	HKMA Outsourcing Guidelines, Section 2.3 IA Outsourcing Guidance, Section 17

Review, monitoring and control	Banks must have controls in place (e.g. comparisons with target service levels) to monitor the performance of CSPs on a continuous basis. Banks must ensure that they have effective procedures for monitoring the performance of, and managing the relationship with, the CSP and the risks associated with the outsourced activity. After the Insurer implements a new outsourcing arrangement or renews or varies an existing outsourcing arrangement, it must re-perform the risk assessment regularly (see due diligence for more information).	HKMA Outsourcing Guidelines, Sections 2.3.2, 2.6.1, 2.6.2 IA Outsourcing Guidance, Section 15
Audit	Banks must ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA and that Data retrieved from the CSPs are accurate and available in Hong Kong on a timely basis. Access to Data by the HKMA's examiners and the Bank's internal and external auditors must not be impeded by the outsourcing. Insurers must ensure that the Cloud Contract allows access by the auditors and actuaries of the Insurer and the IA to any books, records and information.	HKMA Outsourcing Guidelines, Section 2.8 IA Outsourcing Guidance, Section 19
Confidentiality and security	Banks must ensure that the CSP has in place adequate security measures to protect their Data. Banks must have controls in place to ensure that the requirements of Customer Data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of Customer Data. Detailed guidelines must be followed as set out in the HKMA Technology Guidelines. Insurers must ensure that the proposed outsourcing arrangement complies with relevant statutory requirements (e.g. PDPO) and common law customer confidentiality. Insurers must have controls in place to ensure that the requirements of Customer Data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of Customer Data.	HKMA Outsourcing Guidelines, Sections 2.2, 2.5.1 and 2.5.2 IA Outsourcing Guidance, Sections 13 and 21 HKMA Technology Guidelines

Resilience and business continuity	Banks must develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the CSP. Contingency plans must be maintained and regularly tested by Banks and their CSPs to ensure business continuity, e.g. in the event of a breakdown in the systems of the CSP or telecommunication problems with the host country. Insurers must develop a contingency plan to ensure that its business would not be disrupted as a result of undesired contingencies (e.g. systems failure) of the CSP. This must also include procedures to be followed (and the people responsible for respective activities) if business continuity problems arise.	HKMA Technology Guidelines, Section 7.1.1 HKMA Outsourcing Guidelines, Sections 2.7.1 and 2.7.2 IA Outsourcing Guidance, Section 26
Data location	Outsourcing can be to a CSP in Hong Kong or overseas. Banks must give notice to Customers of significant outsourcing initiatives, particularly where the outsourcing is to an overseas jurisdiction. Banks must not outsource to a jurisdiction which is inadequately regulated or which has secrecy laws that may hamper access to Data by the HKMA or a Bank's external auditors. Banks must ensure that the HKMA has right of access to Data. Insurers must understand the risks arising from overseas outsourcing, taking into account relevant aspects of an overseas jurisdiction (e.g. legal system, regulatory regime, sophistication of technology, infrastructure and the ability of the Insurers to monitor the Cloud Services and the CSP).	HKMA Technology Guidelines, Section 2.5.3 and 2.9.1. IA Outsourcing Guidance, Section 28
Data use	Data must not be used for other purposes by the CSP without the consent of the FSI.	HKMA Outsourcing Guidelines, Section 2.5.1 IA Outsourcing Guidance, Section 21 PDPO, Principle 3
Data segregation	Banks must ensure that safeguards for Customer Data confidentiality include segregation or compartmentalisation of the Bank's Data from that of the CSP and its other customers.	HKMA Outsourcing Guidelines, Section 2.5.2

Subcontracting	Banks must include in the Cloud Contract a notification or an approval requirement for significant subcontracting of services and a provision that the original technology CSP is still responsible for its subcontracted services. Insurers must include in the Cloud Contract rules and restrictions on subcontracting e.g. requiring the Insurer's prior consent for the subcontracting and making the CSP liable for the capability of the subcontractor. The Insurer must ensure that its CSP would not engage in subcontracting arrangements which may impede its ability to carry out the provisions of the Cloud Contract with the Insurer, in particular, the requirements on confidentiality, contingency planning and information access right by the Regulator.	HKMA Technology Guidelines, Section 7.1.1 IA Outsourcing Guidance, Section 30
Termination	In the event of a termination of the Cloud Contract, for whatever reason, FSIs must ensure that all Data is either retrieved from the CSP or destroyed.	HKMA Technology Guidelines, Section 2.5.4 IA Outsourcing Guidance, Section 22

4. India[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.[2]
Who are the relevant Regulators?	The Reserve Bank of India (www.rbi.org.in) (**"RBI"**) regulates FSIs. It lays down the legal framework for outsourcing of financial services, including the use of Cloud Services. The Department of Electronics and Information Technology (www.deity.gov.in) (**"DeitY"**) is responsible for policy and administrative decisions related to information technology. An FSI or CSP may be regulated by DeitY as an 'intermediary'. The Department of Telecom (www.dot.gov.in) (**"DoT"**) regulates telecommunications related matters. It regulates FSIs only to the extent they obtain and use telecom resources in India for the provision of IT-enabled financial services.
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No. FSIs intending to use Cloud Services are not required to obtain the RBI's approval. It is entirely up to the FSIs to take a view on the desirability of Cloud Services, after considering the relevant factors outlined in Section C. Notification. FSIs must notify the RBI in situations where Data pertaining to the FSI's Indian operations is stored or processed in another jurisdiction.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No. FSIs wishing to outsource financial services can do so without the need for any approval. There is no form/questionnaire required to be completed, but FSIs can use illustrative checklists prepared by the RBI.

1) Prepared with assistance from Trilegal (www.trilegal.com).

2) The use of Cloud Services by insurance companies in India is regulated by different Regulations, which are not cited in this report. These regulations enumerate the specific types of activities that can be outsourced by insurance companies and the reporting obligations applicable to them. However, there are no material differences with the information provided in this annex for banks.

	FSIs must exercise due diligence before entering into an out-sourcing arrangement and comply with the requirements outlined in Section C.
Are there specific contractual requirements that must be adopted?	Yes. The Cloud Contract must have specific clauses relating to confidentiality, auditing, monitoring, termination, performance standards, dispute resolution, subcontracting and customer rights etc.. See Section C for specific examples.
Other information/developments	The Regulations mentioned in Section B are generally applicable to FSIs. However, certain additional obligations may be imposed on specific types of FSIs such as credit/debit card issuing banks or credit information companies.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks	Outsourcing Guidelines	RBI	RBI/2006/167 DBOD.NO.BP. 40/ 21.04.158/ 2006-07
Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds	Information Security Guidelines	RBI	RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11
Information Technology Act, 2000	IT Act	N/A	9th June, 2000/ Jyaistha 19, 1922 (Saka)
Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011	Privacy Rules	DeitY	GSR 313(E), dt 11-4-2011
Information Technology (Intermediaries Guidelines) Rules, 2011	Intermediary Guidelines	DeitY	GSR 314(E), dt. 11-4-2011

Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks	Credit Cards Circular	RBI	RBI/2014-15/58 DBOD. No.FSD.BC.02/ 24.01.009/2014-15
Credit Information Companies (Regulation) Act, 2006 and Credit Information Companies Rules, 2006	Credit Information Companies Act and Rules	N/A	G.S.R.754 (E). dt. 14-12-2006
Other Service Providers (Terms and Conditions)	OSP Terms	DoT	No.18- 2/2008-CS-I dt. 5-08-2008

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must carry out a risk assessment analysis and due diligence on the CSP to ensure that: • key risks in outsourcing are adequately managed (strategic, reputational, operational, legal, exits, counter-party, country-specific, contractual, access-related, concentration and systemic); • the CSP's capabilities are thoroughly evaluated; • core management functions are not outsourced; • supervision by Regulators and rights of a Customer against the FSI are not affected by the arrangement; • internal control, business conduct or reputation of the FSI is not compromised; and • a comprehensive outsourcing policy is implemented. If a CSP or FSI is regarded as an 'intermediary' under the IT Act, it must observe certain due diligence requirements. An intermediary must publish a privacy policy and user agreement on its website, informing users not to engage in certain activities listed in the Intermediary Guidelines, and also implement a takedown process for unlawful content.	Outsourcing Guidelines, Paras 1.3, 1.5, 2, 4.3, 4.4, 4.5, 5.1, 5.2, 5.3, 5.4, 7.1 and 7.2 of the Annexure Information Security Guidelines, Chapter 1, 2 4, 5, 7, 8 and 9 Intermediary Guidelines, Rule 4

	It is required to inform the Indian Computer Emergency Response team in the case of any cyber security incidents and must appoint a Grievance Officer to address complaints from users. The Intermediary Guidelines also state that an FSI must not knowingly deploy, install or modify the technical configuration of any computer resource to change the course of its operations.	
Review, monitoring and control	FSIs must be able to monitor and control the CSP's activities by: • retaining ultimate control, and being responsible for actions of the CSP; • ensuring that the Board and Senior Management is responsible for core management functions; • clearly defining the outsourced activities, enabling access to all relevant information and creating a management structure to monitor the CSP; • ensuring that access to Customer Data by the staff of the CSP is on a 'need-to-know' basis; • reviewing and monitoring the CSP's security practices and control process and conducting an annual review of its financial and operational conditions; and • if the CSP is not a subsidiary of the FSI, it must not be owned or controlled by any director or officer/employee of the FSI or their relatives.	Outsourcing Guidelines, Paras 2, 4.1, 4.6, 5.2, 5.5.1, 5.6.2 and 5.9 of the Annexure Information Security Guidelines, Chapter 2, 4, 5 and 6 Credit Cards Circular, Paras 8 and 15
Audit	The Cloud Contract must not interfere with the ability of the RBI or FSI to carry out its supervisory functions. It must provide rights to the FSI to conduct audits on the CSP and allow the RBI to access the FSIs documents, records or information stored or processed by the CSP. FSIs engaged in offshore outsourcing of financial services must perform certain additional obligations. FSIs engaged in the outsourcing of services to foreign CSPs must proactively evaluate the economic, social and political risks present in the country to which the services are being outsourced, which may adversely affect the FSI's business and operations. FSIs must carefully consider the enforceability of confidentiality clauses in that jurisdiction and the presence of any regulatory or administrative constraints that could interfere with regular	Outsourcing Guidelines, Paras 2, 4.4, 5.5.1, 5.9 and 7.4 of the Annexure Information Security Guidelines, Chapter 4 and Chapter 5

	audits. It is expected to notify the RBI where inspection or auditing rights may be affected. FSIs must review the applicable data protection and cross-border regulations that would apply to its Customer Data and review the applicability in the case of any significant changes in the services performed by the CSP. FSIs are required to submit an Annual Compliance Certificate to the RBI, with details of all outsourcing contracts, relevant audit periods, major findings of the auditors and countermeasures adopted by it.	
Confidentiality and security	FSIs and CSPs must protect Personal Data by implementing the practices and policies prescribed under the Privacy Rules. An FSI or CSP that is regarded as an 'intermediary' under the IT Act must also publish a privacy policy on its website with a clear explanation of its collection, storage, processing and disclosure practices. The Cloud Contract must have the following provisions on confidentiality and security: • the CSP is liable in the case of any security breach or leakage of information; • the confidentiality obligations imposed on the CSP must continue post-termination; • access to Customer Data by staff of the CSP must be on a 'need to know' basis; and • 128-bit SSL encryption must be used. FSIs are required to notify the RBI in the event of any security breach and CSPs/FSIs are required to report cyber security incidents to the Indian Computer Emergency Response Team. Credit information companies are required to observe specific privacy principles relating to Customer Data.	Privacy Rules, Rule 4 and Rule 8 Outsourcing Guidelines, Paras 4.1, 5.5.1 and 5.6 of the Annexure Information Security Guidelines, Chapter 2 and Chapter 4 Intermediary Guidelines, Rule 4 Credit Information Companies Act, Chapter VI and Credit Information Rules, Chapter III, IV, V and VI Credit Cards Circular, Paras 6.1, 6.2 and 15
Resilience and business continuity	FSIs must require CSPs to establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. FSIs must have contingency plans in place to ensure business continuity, including availability of alternative CSPs.	Outsourcing Guidelines, Paras 5.8 and 5.6.3 of the Annexure Information Security Guidelines, Chapter 4 and Chapter 7

Data location	There is no prohibition on transferring Personal Data outside India, provided that FSIs have put in place safeguards (including contractual measures) to ensure that the CSP protects such information at a standard comparable to that required under the Privacy Rules. However, all original hard-copy records provided by the FSI to the CSP must be maintained in India. If the outsourcing activity involves extensive Data sharing across countries, FSIs may be required to inform the RBI, especially when Data pertaining to Indian operations is stored/ processed abroad. The Information Security Guidelines do not explain the phrase 'extensive data sharing' or 'where the scale and nature of functions outsourced are significant'. However, an FSI is required to notify the RBI in all situations where Data pertaining to its Indian operations are stored or processed abroad.	Privacy Rules, Rule 3 and Rule 7 Outsourcing Guidelines, Paragraph 7.4 of the Annexure Information Security Guidelines, Chapter 4
Data use	CSPs must not use the Data provided by the FSI other than for the purpose it is collected, or is necessary to provide the service. The CSP must not disclose such information. The Cloud Contract must provide for the preservation of documents and Data as legally required, but sensitive personal information must not be retained for longer than required under law.	Privacy Rules, Rule 5 and Rule 6 Outsourcing Guidelines, Paragraph 5.5, of the Annexure
Data segregation	FSIs must ensure that the CSP is able to isolate and clearly identify the FSI's Customer Data, documents, records and assets, and build in strong safeguards so that there is no comingling of such Data or assets.	Outsourcing Guidelines, Paragraph 5.6.3 of the Annexure Information Security Guidelines, Chapter 2 and Annexure A
Subcontracting	The CSP may use subcontractors for all or part of an activity only after obtaining the prior approval of the FSI. The FSI must retain similar control and oversight over such subcontractors.	Outsourcing Guidelines, Paragraph 5.5.1 of the Annexure Information Security Guidelines, Chapter 4
Termination	FSIs must have appropriate termination provisions, including a lock-in period if required. FSIs must take into account the social, economic, political and legal climate of the jurisdiction to which it wishes to outsource services, and include appropriate contingency and exit strategies. If an FSI terminates the services of the CSP, it must inform the Indian Banks' Association along with reasons for the termination. Confidentiality of Customer Data must be maintained even after termination of the Cloud Contract.	Outsourcing Guidelines, Paragraph 5.5, 6 and 7 of the Annexure Information Security Guidelines, Chapter 2 Privacy Rules, Rule 5

5. Indonesia[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Financial Services Authority of Indonesia (www.ojk.go.id/en/, Otoritas Jasa Keuangan) ("**OJK**").[2] Ministry of Communication and Information Technology (www.kominfo.go.id, Kementerian Komunikasi dan Informatika Republik Indonesia) ("**Menkominfo**").
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	Yes.
Is there a process to follow? If so what is the process and is there a specific form/ questionnaire to be completed?	Yes. FSIs[3] must report on any intended outsourcing arrangements to the OJK and obtain approval. Cloud Services would be considered outsourcing arrangements subject to this approval requirement. FSIs must complete and submit a report to OJK as part of the approval process which includes various letters and plans. The content of report must conform with the information sheet as set out in Annex 2 to BI Circular Letter 9/30/DPNP.
Are there specific contractual requirements that must be adopted?	Yes. The OJK mandates contractual requirements that must be agreed by FSIs with CSPs. These can be found in various Sections of the BI Regulation 9/2007 and also in BI Circular Letter 9/30/ DPNP. See Section C for some examples.
Other information/developments	As a result of the OJK taking over the responsibilities of BI, it is expected that the OJK may make changes to the Regulations or issue new Regulations in due course. No timetable or details are available at the current time.

1) Prepared with assistance from Bagus Enrico & Partners (bepartners.co.id).

2) The OJK took over the responsibilities of The Central Bank of Indonesia ("BI") as of 31 December 2013 as the government agency which regulates and supervises FSIs.

3) For the purposes of this Indonesia Annex: (i) FSIs constitute banks which are not public service companies. This is important because banks which are public service companies will be subject to additional rules from October 2017. These additional rules are not considered in this Report; and (ii) FSIs does not include institutions which are not banks e.g. insurance companies.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
Bank Indonesia Regulation 9/15/PBI/2007 on Implementation of Risk Management in the Use of Information Technology by Commercial Banks	BI Regulation 9/2007	OJK	9/15/PBI/2007
BI Circular Letter No. 9/30/DPNP dated 12 December 2007, which can be viewed as the implementing guidelines to BI Regulation 9/2007[1]	BI Circular Letter 9/30/DPNP	OJK	9/30/DPNP
Indonesian Banking Law	Law No. 10 of 1998	OJK	Law No. 10 of 1998
Law No. 11 of 2008 on Electronic Transaction and Information	ITE Law	Menkominfo	Law No. 11 of 2008
Government Regulation No. 82 of 2012 on Electronic System and Transaction	GR No. 82 of 2012	Menkominfo	GR No. 82/2012

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must carry out a selection process with reference to the OJK's own guidelines on outsourcing, as well as FSI's own internal policies and procedures. FSIs' selection process and due diligence must, amongst others, consider: (a) the CSP's qualifications, background and reputation; (b) the financial condition of the CSP; (c) the capability and effectiveness of the CSP; (d) the technology and system architecture; (e) the internal control environment; (f) compliance with existing laws and regulations; and (g) insurance cover.	Annex 1 to BI Circular Letter 9/30/DPNP, Chapter II, Section 2.3(c) Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.2.3

1) Only the Annex 1 which contains the detailed guidelines is available in English and not the appendix which includes the information sheet which must be completed, as explained in Section A.

Review, monitoring and control	FSIs must monitor the Cloud Service provided by the CSP by using a procedure which at least includes service surveillance, error reporting and documentation related to service delivery. CSP must submit to the FSI its (a) annual audited financial report and (b) periodical assessment report conducted by an independent party on Cloud Service facilities.	Annex 1 to BI Circular Letter 9/30/DPNP, Chapter I, Section 3.3.12 See also BI Regulation 9/2007, Article 18 Paragraph (2) Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.3.1(p)
Audit	Internal and external auditors of the FSI and the OJK must be able to obtain Data as demanded.	Annex 1 to BI Circular Letter 9/30/DPNP, Chapter IX, Section 9.4 See also BI Regulation 9/2007, Article 18 Paragraph (2)(a)(5)
Confidentiality and security	The CSP must guarantee the security the FSI's Data.	BI Regulation 9/2007, Article 18 Paragraph (2)(b)(4)
Resilience and business continuity	The CSP must be able to provide disaster recovery and business continuity. The CSP and FSI must have an agreement to store source code program (escrow agreement) for applications with high risk exposure, if CSP does not possess the source code of the relevant application program. If both FSI and CSP do not own the source code of the program, CSP must ensure that the continuity of the application is supported by the software developer principal.	Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.2.3(k) Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.4.2.1
Data location	FSIs cannot place DCs in a jurisdiction where access to information by OJK or other parties appointed by OJK to act on behalf of OJK can be obstructed by legal or administrative restrictions. FSIs may only enter into Cloud Contracts with other parties which operate in a jurisdiction which generally supports the Cloud Contract and agreement of confidentiality. FSIs must notify OJK if there are authorities out of Indonesia which request access to the FSIs' Data or if a situation arises where the right of access of the FSI or OJK to Data is restricted or refused.	Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.4(f) Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.4(d) Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.4(h)
Data use	Data must only be accessible by the FSI.	Appendix 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.3.1(d)

Data segregation	There are no specific requirements.	N/A
Subcontracting	CSPs may subcontract part of their services only with a written agreement of the FSI and with a contract with the subcontractor.	BI Regulation 9/2007, Article 18 Paragraph (2)(b)(5)
Termination	FSIs must have the ability to terminate their Cloud Contract early. The OJK must also be able to terminate the Cloud Contract in the event of any obstruction to conduct an assessment on the DCs/CSP.	BI Regulation 9/2007, Article 18 Paragraph (2)(b)(9) Annex 1 to BI Circular Letter 9/30/DPNP, Chapter X, Section 10.3.4(i)

6. Japan[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Financial Services Agency (www.fsa.go.jp/en/, 金融庁) (**"FSA"**) is responsible for overseeing FSIs.[2] The Centre for Financial Industry Information Systems (www.fisc.or.jp/english/, 金融情報システムセンター) (**"FISC"**).
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No. There are no specific forms or questionnaires that an FSI must complete when considering adopting Cloud Services.
Are there specific contractual requirements that must be adopted?	Yes. The FSA mandates contractual requirements that must be agreed by FSIs with CSPs. These are not set out in one list in any one place but scattered across the different regulations referred to in Section B.
Other information/developments	The FISC has stipulated certain requirements relating to Cloud Services in its standards. Since April 2014, the FISC has been examining the use of Cloud Service by FSIs and it is expected that the FISC will proceed with the revision of certain requirements to promote Cloud Services adoption. The FSA's documents also refer to the FISC's standards and therefore FSIs are advised to comply with them.

1) Prepared with assistance from Anderson Mori & Tomotsune (www.amt-law.com).

2) Note, in Japan, banks, insurance companies and securities companies are subject to separate regulation. For Japan, this report only covers banks and insurance companies.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
The Act on the Protection of Personal Information	APPI	The Consumer Affairs Agency	Act No. 57 of May 30, 2003
The Banking Act	Banking Act	FSA	Act No. 59 of June 1, 1981
Comprehensive Guidelines for Supervision of Insurance Companies	Insurance Guideline	FSA	N/A
Comprehensive Guidelines for Supervision of Major Banks	Banks Guidelines	FSA	N/A
Guidelines for Personal Information Protection in the Financial Field	PI Guidelines	FSA	N/A
Inspection Manual for Insurance Companies	Insurance Manual	FSA	N/A
The Inspection Manual for Deposit-Taking Institutions	Banks Manual	FSA	N/A
FISC Security Guidelines on Computer Systems	FISC Guidelines	FISC	N/A

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must carry out a risk assessment. In summary, this must include: risk identification; analysis and quantification of the potential impact and consequences of these risks; risk mitigation and control strategy; and ongoing risk monitoring and reporting. FSIs must specifically examine the possible risks to their own Customers. FSIs must have defined procedures to select a CSP. FSIs must consider: (a) whether the CSP can provide a sufficient level of	Section II and III of the Banks Guidelines Section II and III of the Insurance Guidelines Section II of the Insurance Manual Section XIV of the FISC Guidelines

	services; (b) whether the CSP's finance position and operations are capable of securing the provision of the services and bearing possible losses in accordance with the Cloud Contract; and (c) any reputational issues e.g. relationship between the CSP and and anti-social forces.	
Review, monitoring and control	The CSP must promptly provide to the FSI appropriate information, as required, in addition to periodic reports regarding the services. The Cloud Contract must specify the contents of the periodic reports to be provided by the CSP to the FSI in relation to the services. The Cloud Contract must include provisions that concern supervision, monitoring and reporting. CSPs must have a procedure in place to report any problems to the FSI.	Section III of the Banks Guidelines and Sections II and III of the Banks Manual Section II of the Insurance Guidelines and Sections II and III of the Insurance Manual
Audit	The Cloud Contract must specify audit rights. The CSP must regularly subject its operations to audits and report the audit results to the FSI.	Section III of the Bank Guidelines and Section III of the Bank Manual Section II of the Insurance Guideline and Section III of the Insurance Manual
Confidentiality and security	The CSP must have a system in place to promptly report to the FSI if there has been a security breach or a system problem. The Cloud Contract must include confidentiality obligations. The CSP must ensure security with regard to the following: (a) physical security, including prevention of physical intrusion and crime prevention; (b) logical security, including measures to protect electronic intrusion; (c) prevention of unauthorised use; (d) computer viruses; and (e) fire, earthquake and flooding. The CSPs systems must be protected through measures such as the use of a password system for access, an identification system and encoding. The CSP must ensure that its staff are aware of the importance of the confidentiality of the Data.	Sections I, II and III of the Banks Guideline and Sections I, II and III of the Bank Manual Section III of the Insurance Guidelines and Sections I, II and III of the Insurance Manual
Resilience and business continuity	The Cloud Contract must specify the backup obligations and the the failure and disaster recovery routines. FSIs must set a recovery target for the CSP. FSIs and the CSPs must test the contingency plans of the CSP. FSIs must ensure that there is a contingency plan in place which includes arrangements and procedures for dealing with emergencies, natural disasters, terrorism and IT issues. FSIs and CSPs must conduct training on the contingency plans.	Section XIV of the FISC Guidelines Sections II and III of the Bank Guideline and Sections II and III of the Bank Manual Section II of the Insurance Guideline and Section III of the Insurance Manual

	FSIs must ensure that the Cloud Services will not cause serious problems to its business or its Customers if the Cloud Services are not provided. The FSI must ensure that there are appropriate back-up measures. The back-up measures must avoid geographic concentration.	
Data location	There are no specific requirements.	N/A
Data use	The Cloud Contract must include prohibitions on unintended use of the Data by the CSP.	Section III of the Bank Guideline and Section II of the Bank Manual Section II of the Insurance Guideline and Section III of the Insurance Manual
Data segregation	There are no specific requirements.	N/A
Subcontracting	The CSP must adequately supervise subcontractors. The Cloud Contract must specify the subcontracting procedures.	Sections II and III of the Banks Guidelines Section III of the Insurance Guidelines Section XIV of the FISC Guidelines
Termination	The FSI must be able to terminate the Cloud Contract where necessary. The Cloud Contract must specify the termination rights and that the Data must be deleted by the CSP on termination.	Section II of the Banks Manual Section II of the Insurance Manual Section XIV of the FISC Guidelines

7. Malaysia[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Bank Negara Malaysia (www.bnm.gov.my) (**"BNM"**).[2] The Personal Data Protection Commission (www.pdp.gov.my/index.php/en) (**"PDPC"**).
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	Yes if overseas. The prior consent of BNM is required if an FSI wishes to outsource to an overseas CSP. Notification only for other outsourcing. All outsourcings must be notified to BNM.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No. There are no specific forms or questionnaires that an FSI must complete when considering Cloud Services.
Are there specific contractual requirements that must be adopted?	Yes. BNM does specifically mandate contractual requirements that must be agreed by FSIs in their Cloud Contracts. These are not set out in one list in any one place but scattered across the different documents referred to in Section B.
Other information/developments	N/A

1) Prepared with assistance from ZUL RAFIQUE & Partners (www.zulrafique.com.my).
2) Banks and Insurers are subject to some different BNM Regulations. Some of the relevant differences are set out in Section C.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
BNM's Guidelines on Outsourcing for Insurers.	BNM Outsourcing Guidelines (Insurers)	BNM	N/A
BNM's Guidelines on Internet Insurance	BNM Internet Insurance Guidelines	BNM	N/A
BNM's Guidelines on Data Management and MIS Framework	BNM Data Management Guidelines	BNM	N/A
BNM's Guidelines on Business Continuity Management	BNM BCM Guidelines	BNM	N/A
BNM's Guidelines on Management of IT Environment	BNM IT Management Guidelines	BNM	N/A
BNM's Guidelines on Outsourcing of Banking Operations	BNM Outsourcing Guidelines (Banking)	BNM	N/A
BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services	BNM E-Banking Guidelines	BNM	N/A
Financial Services Act 2013 / Islamic Financial Services Act 2013	FSA/IFSA	BNM	Act 758 / Act 759
Personal Data Protection Act 2010	PDPA	PDPC	Act 709

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must perform a due diligence review on the capabilities and expertise of the CSP prior to selection. Due diligence must be adequately carried out to review and assess outsourcing viabilities, capabilities, reliabilities, expertise and track records before being approved by the board of directors. The board and senior management of the FSI must ensure that an appropriate due diligence review of the competency, system infrastructure and financial viability of the CSPs is conducted prior to entering into any contract for e-banking services.	Paragraph 47.1(i) of the BNM Outsourcing Guidelines (Banking) Paragraph 15(a), Part II of the BNM IT Management Guidelines Paragraph 10.4 of the BNM Outsourcing Guidelines (Insurers) Paragraph 13.3(b) of the BNM E-Banking Guidelines
Review, monitoring and control	Banks must have in place comprehensive and ongoing due diligence and oversight process for managing the FSI's outsourcing relationship and other third-party dependencies supporting e-banking. FSIs must have in place effective oversight, review and reporting arrangements to ensure that standards on Data quality, integrity and accessibility are observed at all times. FSIs must have proper reporting and monitoring procedures over the integrity and quality of work conducted by a CSP. Insurers must have appropriate oversight framework to monitor the outsourcing vendor's controls, condition and performance, and proper reporting and monitoring mechanisms over the integrity and quality of work by the outsourcing vendor. Insurers must develop and implement procedure to monitor and control outsourcing arrangements to ensure that the services are being delivered in the manner expected and in accordance with the terms of the service agreement, and associated risks are being effectively managed.	Paragraph 13 of the BNM E-Banking Guidelines Paragraph 47.1(vi) of the BNM Outsourcing Guidelines Paragraph 4.12 of the BNM Data Management Guidelines Paragraphs 26.1(c) and (d) of the Internet Insurance Guidelines Paragraph 10.14 of the BNM Outsourcing Guidelines (Insurers)

Audit	CSPs must provide FSIs and the BNM with a right of audit. The external and internal auditors of the FSI must be able to review the books and internal controls of the CSPs.	Section 148(1)(c) of the FSA / 160(1)(b) of the IFSA Paragraph 4(viii) of the BNM Outsourcing Guidelines Paragraph 13.3(f) of the BNM E-Banking Guidelines Paragraph 15(c), Part II and Paragraph 1(c), Part V of the BNM IT Management Guidelines Paragraph 113 of the BNM BCM Guidelines Paragraph 26.1 (e) of the BNM Outsourcing Guidelines (Insurers) Paragraph 10.10(i) of the BNM Outsourcing Guidelines (Insurers)
Confidentiality and security	Banks must obtain from the CSP a written undertaking to protect and maintain the confidentiality of their Data. FSIs must ensure that adequate internal controls, prevention measures and early detection of fraud, errors, omissions and other irregularities are in place. CSPs must implement specific security practices contained in the BNM IT Management Guidelines. CSPs must implement proper security precautions to ensure that transfers of Data are not monitored or read by any unauthorised parties and Data storage systems are well protected. FSIs should evaluate the ability of the CSPs to maintain at least similar or more stringent level of security. FSIs should also adopt more rigorous monitoring and control to ensure adequate protection of information is maintained. All outsourcing arrangements should be coordinated to ensure that confidentiality, integrity and availability of information is not compromised. Insurer must ensure that the ownership and control of the insurer's records remains with the insurer and the CSPs is to provide the insurer with a written undertaking on its compliance with secrecy of customers' and the insurer's information; and the vendor is also to abide by any data protection legislation that is in effect.	Section 133(1) of the FSA / 145(1) of the IFSA Section 9 of the PDPA Paragraph 47.1(iii) of the BNM Outsourcing Guidelines (Banking) Paragraphs 13.3(d) and (e) of the BNM E-Banking Guidelines Paragraph 15(b)of Part II of the BNM IT Management Guidelines Paragraph 26.1(f) and (g) of the BNM Internet Insurance Guidelines Paragraph 10.10(e) of the BNM Outsourcing Guidelines (Insurers)

	Insurer must ensure that the service agreements with the CSPs shall contain obligations of the CSPs to protect confidential information, including provisions prohibiting the CSPs and its agent from using or disclosing the insurer's proprietary information or that of its customers, except as necessary to provide the contracted services and to meet regulatory and statutory provisions.	
Resilience and business continuity	CSPs and FSIs must have fully documented and adequately resourced business continuity plans and disaster recovery plans. These must address reasonably foreseeable situations where the CSP fails to provide the required services, causing disruptions to the FSI's operations. FSIs must ensure that periodic testing is conducted by the CSPs on these plans, at least annually (in the case of business continuity plans) and twice a year (in the case of disaster recovery plans). FSIs must ensure that appropriate contingency plans for outsourced e-banking activities are in place. All service agreements should contain contingency arrangements outlining the CSPs' measures for ensuring the continuation of the outsourced activity in the event of problems affecting the CSPs' operation. The agreement should place an obligation on the CSPs to regularly test its business resumption and contingency systems and to notify the insurer of the test results. In addition, the insurer should be notified in the event that the CSP makes significant changes to its contingency plans.	Paragraphs 112 and 115 of the BNM BCM Guidelines Paragraph 13.3(g) of the BNM E-Banking Guidelines Paragraph 10.10(g) of the BNM Outsourcing Guidelines (Insurers) Paragraph 4(ix) of BNM Outsourcing Guidelines (Banking)
Data location	Personal Data may be transferred outside of Malaysia where, amongst other exceptions, the relevant individual has consented to such transfer or the transfer is necessary for the performance of a contract between the FSI and the relevant individual or the CSP has taken all reasonable precaution and exercised all due diligence to ensure that the Personal Data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA.	PDPA, Section 129
Data use	CSPs must not use Personal Data for any purpose other than the purpose for which the Personal Data was collected except in limited circumstances (e.g. the relevant individual has given his consent to the disclosure or the disclosure is necessary for the prevention or detection of a crime, or for the purpose of investigations or authorised by law or any order of the court).	PDPA, Sections 8 and 39

Data segregation	The CSP must be able to isolate and clearly identify the FSI's Data, documents, records and assets to protect their confidentiality.	Paragraphs 20.2 and 20.3 of the BNM E-Banking Guidelines Paragraph 15(b), Part II of the BNM IT Management Guidelines Paragraphs 10.10(c) and (e) of BNM Outsourcing Guidelines
Subcontracting	The CSP must obtain the approval of the FSI before using subcontractors and the FSI must ensure that the conditions for subcontracting allow the FSI to maintain similar controls over the outsourcing relationship and outsourcing risks as if the Cloud Service were not subcontracted.	Paragraph 10.10(k), BNM Outsourcing Guidelines (Insurers)
Termination	FSIs must have appropriate exit provisions in the Cloud Contract with the CSP. The provisions must include exit provisions which lay down clear procedures for the return of the Data in a timely manner, in the event of default or termination	Paragraph 4(v) of the BNM Outsourcing Guidelines (Banking) Paragraphs 10.6 and 10.10(i) of the BNM Outsourcing Guidelines (Insurers)

8. New Zealand[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Reserve Bank of New Zealand (www.rbnz.govt.nz) (**"RBNZ"**) regulates FSIs The Privacy Commissioner (www.privacy.org.nz) (**"PC"**) regulates the use of Personal Data (including by FSIs).
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No. The RBNZ does not require approval before FSIs in New Zealand outsource certain IT functionality to a CSP.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No. There are no specific forms, questionnaires or processes that an FSI must complete or follow when considering Cloud Services.
Are there specific contractual requirements that must be adopted?	No. The RBNZ does not stipulate any mandatory contractual requirements that FSIs must ensure are included in their Cloud Contracts.
Other information/developments	The PC has created a document called 'Cloud Computing: A guide to making the right choices', February 2013 which contains some useful items to check. The Cloud Computing Code of Practice is a voluntary, disclosure-based code of practice to which CSPs may sign up. It requires signatories to disclose details of their cloud products and services.

1) Prepared with assistance from Buddle Findlay (www.buddlefindlay.com).

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
RBNZ Outsourcing Policy of January 2006[1]	RBNZ Outsourcing Policy	RBNZ	BS 11
Privacy Act 1993	Privacy Act	PC	1993 No. 28

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must satisfy themselves that their arrangements or any proposed arrangements are adequate, especially where a core function is involved.	RBNZ Outsourcing Policy, Section 37
Review, monitoring and control	FSIs must have the legal and practical ability to control and execute any business, and any functions relating to any business, of the FSI that are carried on by a person other than the FSI, sufficient to achieve, under normal business conditions and in the event of stress or failure of the FSI or of a CSP to the FSI, the core functions.	RBNZ Outsourcing Policy, Section 4
Audit	There are no specific requirements.	N/A
Confidentiality and security	FSIs must ensure Personal Data is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss; and access, use, modification, or disclosure, except with the authority of the agency that holds the information; and other misuse.	Privacy Act, Principle 5
Resilience and business continuity	FSIs must establish a credible internal process to manage the risks to its business associated with any outsourcing arrangements which may include business continuity and disaster recovery plans. Outsourcing arrangements must not create risk that the operation and management of the FSI might be interrupted for a material length of time.	RBNZ Outsourcing Policy, Sections 10 and 33

1) Large banks must comply with the RBNZ Outsourcing Policy. RBNZ will consider a bank as "large" if its liabilities net of amounts due to related parties exceed NZD 10 billion. Currently, BNZ, ASB, ANZ National, Kiwibank and Westpac are the only banks that are considered "large".

Data location	There is no prohibition on transferring Personal Data outside of New Zealand unless the transfer would be likely to lead to a contravention of the basic data protection principles of the Privacy Act.	Privacy Act
Data use	CSPs that hold Personal Data that was obtained in connection with one purpose shall not use the information for any other purpose.	Privacy Act
Data segregation	There are no specific requirements.	N/A
Subcontracting	There are no specific requirements.	N/A
Termination	There are no specific requirements.	N/A

9. Philippines[1]

A. Overview

Is the use of Cloud Services permitted?	Yes. However, inherent banking functions may not be outsourced and in the BSP IT Guidelines, the BSP has stated that, at present, it would only allow the use of Public Cloud Services for non-core operations and business processes (e.g. email, office productivity, collaboration tools, claims and legal management).
Who are the relevant Regulators?	Bangko Sentral ng Pilipinas (www.bsp.gov.ph) (**"BSP"**) is the central bank of the Philippines. BSP is responsible for price stability and a balanced and sustainable growth of the economy. Certain entities may also be subject to secondary licensing requirements administered by the Securities and Exchange Commission and/or the Insurance Commission.
Are there specific regulations dealing exclusively with Cloud Services?	No specific regulations but Cloud Computing Questionnaire serves as a single reference for regulations for FSIs procuring Cloud Services. See below for more details.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	Yes. BSP is aware of the general trend of FSIs wishing to use Cloud Services. As a general rule, BSP currently requires institutions under its supervision ("FSIs") to obtain the prior approval of the Monetary Board in order to outsource IT systems and processes.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	Yes. In order to streamline the process of obtaining approval, BSP has issued a "Cloud Computing Questionnaire", which contains a number of questions about an FSI's decision to use Cloud Services. The main purpose of the Cloud Computing Questionnaire is to establish that an organisation has carried out appropriate due diligence and the proposed Cloud Service complies with applicable regulatory requirements in relation to issues such as data security, confidentiality and disaster recovery. FSIs are required to complete this questionnaire as part of the approval process.

1) Prepared with assistance from SyCip Salazar Hernandez & Gatmaitan (www.syciplaw.com).

Are there specific contractual requirements that must be adopted?	Yes. The Cloud Computing Questionnaire contains some questions which ask for confirmation that certain specific items are covered in the Cloud Contract. The BSP Manual of Operation for Banks also provides for mandatory provisions in the Cloud Contract.
Other information/developments	No.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
BSP Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions	BSP IT Guidelines	BSP	Circular No. 808, Series of 2013
BSP Revised Outsourcing Framework for Banks	BSP Outsourcing Frameworks	BSP	Circular No. 765, Series of 2012
Manual of Operation for Banks	BSP Manual of Operation	BSP	N/A
Bank Deposits Secrecy Law	Deposits Secrecy Law	BSP	Republic Act No. 1405
Foreign Currency Deposits Act	Foreign Deposits Secrecy Law	BSP	Republic Act No. 6426
General Banking Law	Banking Law	BSP	Republic Act No. 8791
Anti-Money Laundering Act	AMLA	Anti-Money Laundering Council	Republic Act No. 9160, as amended by Republic Act No. 10365
Credit Information System Act	CISA	Credit Information Corporation	Republic Act No. 9510
Data Privacy Act	DPA	National Privacy Commission	Republic Act No. 10173

Cybercrime Prevention Act	CPA	National Bureau of Investigation; Philippine National Police	Republic Act No. 10175

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	Before selecting a CSP, the FSI must perform appropriate due diligence.	BSP IT Guidelines Appendix 75e, Section 3
Review, monitoring and control	FSIs must have an effective outsourcing oversight program that provides the framework for management to understand, monitor, measure and control the risks associated with outsourcing.	BSP IT Guidelines page 12.
Audit	FSIs must conduct a regular, comprehensive audit of CSPs. The audit scope must include a review of controls and operating procedures that help protect FSIs from losses due to irregularities and wilful manipulations. CSPs must grant BSP access to its cloud infrastructure to determine compliance with applicable laws and regulations and assess soundness of risk management processes and controls in place.	BSP IT Guidelines Appendix 75e, Section 5 BSP IT Guidelines Appendix, 75e, Annex A
Confidentiality and security	Under various banking and finance related laws, bank records are considered absolutely confidential in nature and may not be examined except under certain circumstances. Credit information is likewise strictly confidential. FSIs must ensure that CSPs have strict security measures in place, including for (a) security administration/system access functions; (b) password administration and management; (c) privilege accounts; (d) remote access activities; and (e) change management.	Deposits Secrecy Law, Foreign Deposits Secrecy Law, General Banking Law, Credit Information Law BSP IT Guidelines Appendix 75e, Annex A
Resilience and business continuity	FSIs must ensure the viability of CSPs' business continuity and disaster recovery plans to address broad-based disruptions to its capabilities and infrastructure.	BSP IT Guidelines Appendix 75e, Annex A

Data location	CSP must have some reliable means to ensure that an FSI's Data is stored and processed only within specific jurisdictions. The same safeguards must be in place no matter in which jurisdiction the Data is held.	BSP IT Guidelines Appendix 75e, Annex A
Data use	FSIs must retain exclusive ownership over all their Data and the Data must only be used for its own purposes.	BSP IT Guidelines Appendix 75e, Annex A.
Data segregation	FSIs must pay attention to the CSP's ability to isolate and clearly identify its Data and other information system assets for protection.	BSP IT Guidelines Appendix 75e, Annex A
Subcontracting	CSPs may use subcontractors to the extent that the additional services performed by the subcontractors are limited to peripheral or support functions while the core services must rest with the CSP.	BSP IT Guidelines Appendix 75e, Section 3.3
Termination	FSIs must have the right to terminate the Cloud Contract by contractual notice if the BSP requires that FSI to terminate the Cloud Contract. The BSP also suggests that the Service Level Agreement, which formalizes the performance standards against which the quantity and quality of service should be measured, be linked to provisions in the Cloud Contract regarding termination in order to protect the FSI in the event the CSP fails to meet the required level of performance.	BSP Outsourcing Frameworks, Appendix BSP IT Guidelines Appendix 75e, Section 3.4 and Annex A

10. Singapore

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Monetary Authority of Singapore (www.mas.gov.sg) (**"MAS"**) regulates FSIs. The Personal Data Protection Commission (www.pdpc.gov.sg) (**"PDPC"**) regulates the use of Personal Data (including by FSIs). The Infocomm Development Authority of Singapore (www.ida.gov.sg) (**"IDA"**), a statutory board of the Singapore Government, responsible for the development and growth of the infocomm sector in Singapore.
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No. There is no requirement for approval. However, a completed questionnaire (see below) must be submitted to the MAS before an FSI enters into a "material outsourcing"[1] and the FSI must consult with the MAS. The consultation process can be detailed and thorough. The MAS will care in particular about the security levels provided by the Cloud Services. However, what the consultation process will involve will depend on the type of services the Data to be transferred.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	Yes. The MAS Technology Questionnaire for Outsourcing sets out questions about an FSI's decision to outsource, including its use of Cloud Services. FSIs must submit the completed questionnaire to the MAS before signing up for a material IT outsourcing project. The main purpose of the MAS Technology Questionnaire is to establish that the FSI has carried out appropriate due diligence and that the proposed service complies with applicable regulatory requirements in relation to issues such as Data security, confidentiality and disaster recovery. The MAS may ask the FSI further questions after it has reviewed the completed questionnaire but there is no requirement to wait for an approval from the MAS.

1) Section 5 of the MAS Technology Questionnaire for Outsourcing contains factors impacting 'materiality' which FSIs will need to consider in their assessment.

Are there specific contractual requirements that must be adopted?	Yes. The MAS Technology Questionnaire contains questions that ask for confirmation that certain specific items are covered in the FSI's Cloud Contract with a CSP. Some additional obligations that MAS requires FSIs to ensure are covered in Cloud Contracts are found in the Technology Risk Management Guidelines and Guidelines on Outsourcing. See the table below for some examples.
Other information/developments	In 2013, the IDA published its Multi-Tier Cloud Security Framework. It is a voluntary system of certification for CSPs, with different tiers applying to different categories of Data (i.e. one tier applies to CSPs who deal with non-business critical Data, a higher tier applies to those who deal with business critical Data and the highest tier applies to those who process specific types of sensitive Data, such as FSIs' Data and health records). Whilst adoption of the framework is voluntary, CSPs should anticipate that Singapore-based customers may ask questions about the framework and whether or not the CSP is compliant or is obtaining the certification. In September 2014, the MAS issued a consultation on its proposed new Outsourcing Notice and Guidelines. The consultation suggests that MAS will tighten some of the requirements on outsourcing. The key changes proposed by the MAS relate to: • a more detailed due diligence process, including a requirement to carry out due diligence on the staff of the supplier; • a requirement to report adverse incidents to MAS; and • more detailed requirements covering regular audits and reviews of outsourcing arrangements. It is not yet known, at the time of writing, when the new rules will come into force.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
Banking Act (Section 47)	Banking Act	MAS	Act 41 of 1970
Securities & Futures Act (Section 21)	Securities & Futures Act	MAS	Act 42 of 2001
Notice 634	Banking Secrecy Notice	MAS	MAS 634
Technology Risk Management Guidelines	TRM Guidelines	MAS	N/A
Guidelines on Outsourcing	Outsourcing Guidelines	MAS	N/A
Technology Questionnaire on Outsourcing	MAS Technology Questionnaire	MAS	N/A
Business Continuity Management Guidelines	BCM Guidelines	MAS	N/A
Personal Data Protection Act	PDPA	PDPC	No. 26 of 2012

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must carry out a risk assessment and due diligence on the CSP to ensure that the CSP and its Cloud Services meet legal, regulatory, contractual and business requirements.	Outsourcing Guidelines, Paras 6.2 and 6.3 TRM Guidelines Paras 5.1 and 5.2 MAS Technology Questionnaire Banking Secrecy Notice, Paragraph 2

Review, monitoring and control	FSIs must be able to monitor and control the CSP, including by obtaining regular reporting and information, to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the Cloud Contract. FSIs must regularly review the reports and performance levels. The Cloud Contract must provide a mechanism for remedial actions for any issues that emerge.	Outsourcing Guidelines, Paragraph 6.7 TRM Guidelines, Paragraph 5.1 MAS Technology Questionnaire
Audit	CSPs must provide the MAS and the FSI with a right of audit.	Outsourcing Guidelines, Paragraph 6.8 Banking Secrecy Notice, Paragraph 8 MAS Technology Questionnaire
Confidentiality and security	FSIs must adopt a sound and robust technology risk management framework and consider carefully the use of Cloud Services under the MAS's Technology Risk Management Guidelines. CSPs must maintain robust security measures and comprehensive security policies. CSPs must use encryption technology to protect and secure the FSI's Data at all times.	Outsourcing Guidelines, Paragraph 6.5 TRM Guidelines Banking Act, Section 47 Banking Secrecy Notice MAS Technology Questionnaire PDPA, Section 24
Resilience and business continuity	CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives. CSPs must regularly test and update procedures and systems in place to meet those objectives. The risks of downtime must be minimised through good planning and a high degree of system resilience.	MAS Outsourcing Guidelines, Paragraph 6.6 BCM Guidelines TRM Guidelines MAS Technology Questionnaire
Data location	No prohibition on transferring Personal Data outside of Singapore, provided that FSIs have put in place safeguards (including contractual measures) to make sure that Personal Data is protected to a comparable standard of protection as it is under the PDPA within Singapore. The MAS requires FSIs to know exactly where Data will be located and that FSIs ensure that the government policies, economic and legal conditions of the identified jurisdictions are stable.	PDPA, Section 26 Outsourcing Guidelines, Paragraph 6.9 MAS Technology Questionnaire

Data use	CSPs must not use FSI's Data for any purpose other than that which is necessary to provide the services. The Cloud Contract must prevent CSPs from using FSI Data for any secondary purpose at all times.	Outsourcing Guidelines MAS Technology Questionnaire PDPA, Section 18
Data segregation	FSI Customer Data must be segregated from other Data held by the CSPs. CSPs must be able to identify the FSI's Data and at all times be able to distinguish it from other Data held by the CSP.	Outsourcing Guidelines, Paragraph 6.5 TRM Guidelines, Paragraph 5.2 MAS Technology Questionnaire
Subcontracting	CSPs may only use subcontractors if the subcontractors are subject to equivalent controls as the CSP. Subcontractors must not ordinarily be given access to the FSI's Data.	Outsourcing Guidelines, Paragraph 6.4 MAS Technology Questionnaire PDPA, Section 17.
Termination	FSIs must have appropriate exit provisions in the Cloud Contract. To the extent that the FSI requires, on termination, the CSP must work with the FSI to return the FSI's Data to the FSI and then the CSP must permanently delete the Data from the CSP's systems.	Outsourcing Guidelines, Paragraph 6.4 MAS Technology Questionnaire TRM Guidelines, Paragraph 5.2 PDPA, Section 25.

11. South Korea

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Financial Services Commission (www.fsc.go.kr/eng/, 금융위원회) (**"FSC"**). The Financial Supervisory Services (english.fss.or.kr/fss/en/main.jsp, 금융감독원) (**"FSS"**). The Personal Information Protection Commission (www.pipc.go.kr/cmt/main/english.do, 개인정보보호위원) (**"PIPC"**). The Korea Communications Commission (eng.kcc.go.kr/user/ehpMain.do, 방송통신위원회) (**"KCC"**).
Are there specific regulations dealing exclusively with Cloud Services?	Yes. The Personal Information Protection Rules for Cloud Services. It is recommended that these Rules are followed as KCC guidelines but they are not binding as law. And a new law is expected. See below.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	Use of offshore DCs is prohibited. No approval required for onshore DCs but there is a notification requirement (see below).
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	Yes. The FSI must report to the FSS the fact that the handling of Data is being outsourced to a third party. The FSI must submit a number of documents to the FSS at least seven business days before the conclusion of the Cloud Contract, including a copy of the Cloud Contract, the FSI's internal outsourcing standards, a statement from the FSI's compliance officer that the project does not violate any Regulations, details of any major alterations to the FSI's business conduct procedures and confirmation that the Regulator can supervise the outsourced activities.

	The FSS may request changes or more information to the outsourced activities at any time.
Are there specific contractual requirements that must be adopted?	Yes. The Regulations and the June Regulation prescribe standard contract terms that must be reflected in the Cloud Contract with a CSP. See Section C for examples.
Other information/developments	There is a proposed Act on Promotion of Cloud Computing and User Protection (the "Cloud Act") in Korea. It was submitted to the National Assembly on 16 October 2013 but there is no fixed timeframe for its implementation. Nonetheless, it is worth being aware of as it will make some important changes to the regulation of cloud in Korea. In summary, it provides as follows: • There will be certain special regulatory provisions which recommend that CSPs abide by matters determined and announced by the Minister of Science, ICT and Future Planning, such as the quality/capability of the Cloud Services, appropriate service levels and standards for information protection. Because of this, it is anticipated that an autonomous Cloud Service certification system will soon be implemented. • In order to promote Cloud Services, where a company obtains/equips computer equipment by using Cloud Services, it is deemed that the required approval or permission under the individual laws has been obtained pursuant to the Cloud Act. • With respect to information security and protection of users, according to the Cloud Act, it will be recommended that a standardized contract be used when providing Cloud Services. • The information of a user cannot be provided to a third party or be used for purposes other than the designated purpose without the consent of such user. Further, if a CSP saves the information of the user abroad, the user may request the CSP to provide the name of the country where such user's information is saved. In the case that a user incurs damages due to the deliberate or negligent acts of a CSP which violate the Cloud Act, such user may raise a claim for compensation of damages against such CSP.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
Banking Act	BA	FSC/FSS	Act No. 9784 (Jun. 9, 2009)
Insurance Business Act	IBA	FSC/FSS	Act No. 8902 (Mar. 14, 2008)
Regulations Regarding Outsourcing by Financial Institutions	The Regulations	FSC/FSS	FSC 2005-39
Regulation on Outsourcing of Data Processing and Computer Facilities of Financial Companies	The June Regulation	FSC/FSS	FSC Official Announcement No. 2013-17
The Personal Information Protection Act	PIPA	PIPC	Act No. 11690 (2013.3.23)
The Personal Information Protection Rules for Cloud Services Providers	The Rules	KCC	KCS.KO-10.2001

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must establish and comply with their own outsourcing standards, which must include measures for evaluation of the risks associated with the outsourcing and measures to manage such risks.	The Regulations, Appendix 2
Review, monitoring and control	FSIs must establish a procedure to monitor the financial position of CSPs, risks, emergency measures and tests results for these emergency measures.	The Regulations, Appendix 2
Audit	The FSI must ensure that the FSC and the FSS have the ability to access and audit the CSP and this must be provided for in the Cloud Contract. The FSI must also have a right to audit the CSP in its Cloud Contract with the CSP.	The Regulations, Appendix 2 The June Regulation, Article 8-1 and Table 1

Confidentiality and security	The CSP must take security measures to protect confidential information and must be contractually obliged to do so by the FSI. The CSP must take measures to protect Personal Data, including encryption. The CSP must notify the FSI immediately of any security failure. This must be included in the Cloud Contract.	The Regulations, Appendix 2 The June Regulation, Article 5-1 and Table 1
Resilience and business continuity	The FSI must ensure that there is a plan in place to deal with unforeseen events such as insolvency or telecommunications malfunctions. The CSP must be contractually required to have in place back-up procedures to secure continuity of the service.	The Regulations, Appendix 2
Data location	The use of offshore DCs by FSIs is prohibited. The CSP must take extra care to prevent the transfer of Customer Data to a foreign country.	The June Regulation, Articles 4-1 and 8-1
Data use	The Cloud Contract must state that the Data is owned by the FSI and place conditions on the CSP's use of the Data. The CSP must not be allowed to use the Data for any other purposes beyond providing the services to the FSI. This limitation must be included in the Cloud Contract.	The Regulations, Appendix 2 The June Regulation, Article 4-5 and Table 1
Data segregation	The CSP must separately manage the FSI's information, granting access only to authorised persons.	The Regulations, Appendix 2
Subcontracting	If the CSP is permitted to subcontract, the Cloud Contract must oblige the CSP to ensure compliance with the terms of the Cloud Contract. Where Data has been shared with the CSP, the CSP must not be permitted to subcontract the processing of the Data unless the FSS has acknowledged the subcontracting. The CSP must not further subcontract without the consent of the FSI. This must be included in the Cloud Contract.	The Regulations, Appendix 2 The June Regulation, Article 4-4 and Table 1
Termination	The Cloud Contract must include rights for the FSI to terminate for a violation by the CSP of its obligations and for a violation of any Regulation. The Cloud Contract must include a right for the FSI to obtain its Data from the CSP upon termination.	The Regulations, Appendix 2 The June Regulation, Table 1

12. Taiwan[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	Taiwan's Financial Supervisory Commission (www.fsc.gov.tw/en/index.jsp, 金融監督管理委員會) ("**FSC**") regulates FSIs. The FSC is also the competent authority under the Personal Information Protection Act ("**PIPA**") for the collection, processing, and use of personal information by FSIs. The Ministry of Justice has overall authority for the PIPA. Taiwan's Institute for Information Industry, an NGO established through public and private cooperation, also provides relevant 'guidance' on Cloud Services.
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	Yes, if offshore. If onshore, it depends on the service. The FSC regulates any outsourcing by FSIs, domestic and offshore outsourcing. Different requirements apply to domestic vs. offshore outsourcing, and there are also different regulations for a financial institution (these include domestic banks and their overseas branches, branches of foreign banks in Taiwan, credit cooperatives, bills finance companies, and institutions operating credit card business) ("FIs") vs. insurance institutions ("IIs"). There are nineteen approved services that FIs may outsource by regulation and the FSC has the authority to (and has in the past) added to this list. Offshore outsourcing requires prior special regulatory approval. Outsourcing services domestically can still require prior regulatory approval (or can proceed without prior regulatory approval); this depends on the service being outsourced.

1) Prepared with assistance from Eiger (www.eigerlaw.com).

	Any offshore Cloud Services would require prior regulatory approval. Domestic Cloud Services will depend upon the type of actual service being outsourced as to whether prior approval would be required. The latter was confirmed unofficially with the FSC.
Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	Yes, but there is no form/questionnaire. The Regulations and the Directions set out the relevant processes. Certain domestic outsourcing transactions require approval: e.g. the outsourcing of credit card issuance, marketing of consumer loans other than auto loans, and collection of debts require the prior approval of the competent authority. Generally Cloud Services would not be included within this category. Other domestic outsourcing transactions: No approval required for FIs or IIs. However, the Board of Directors must provide approval internally. Offshore outsourcing: Approval is required for FIs and IIs. FIs and IIs must apply to the FSC for prior approval. Assurances are required from the Regulators in the CSP's jurisdiction (the "Foreign Regulator") on disclosure, examination, and the protection of Data. For FIs: • the Foreign Regulator agrees that the Taiwan Regulator can request the CSP to provide relevant information on the outsourced items; • the Foreign Regulator allows the competent authority in Taiwan and the FI to conduct necessary examinations of the outsourced items; • the Foreign Regulator shall inform the Taiwan Regulator in advance if it plans to examine the outsourced items; and • the Foreign Regulator agrees not to obtain the Data from Taiwan. If it obtains such Data while exercising its supervisory function, it shall inform the Taiwan Regulator in advance. If the above cannot be obtained then there are five additional requirements that must be met by the FI in Taiwan: • a letter of consent from the CSP that a person designated by the FI may examine the outsourced items; • an evaluation on internal control principles and operating procedure of the CSP; • a legal opinion indicating that the protection of Data in the CSP's jurisdiction is not below the protection provided in Taiwan;

- audited financial statements of the CSP for the most recent fiscal year; and
- a statement issued by the CSP certifying that no violation of customer interests, personnel malpractice, information and technology security, and other occurrences have impacted business operations in the last three years.

For IIs: The II shall obtain a letter of consent on supervisory cooperation from the Foreign Regulator. The letter of consent shall contain the following:

- the Foreign Regulator is aware of the matter and agrees to the provision of the Cloud Services by the CSP;
- the Foreign Regulator allows the Taiwan Regulator and the II to conduct necessary examination of the outsourced items; and
- the Foreign Regulator shall inform the Taiwan Regulator in advance if it plans to examine the outsourced items.

Where an II is unable to obtain the letter of consent from the Foreign Regulator, it shall first acquire a letter of consent from the CSP that a person designated by the II may examine the outsourced items.

Are there specific contractual requirements that must be adopted?

Yes. The Regulations and Directives address specific obligations with respect to outsourcing. The FSC PIPA Regulations also set out specific requirements for Personal Data and PIPA compliance.

Other information/developments

The Institute for Information Industry has established a series of guidelines relevant to Cloud Services and Data collection in the financial industry. With regards to the use of Cloud Services, the Institute actively promotes the use of service level agreements.

With regards to the protection of Personal Data collected, the Institute has introduced the Taiwan Personal Information Protection and Administration System (TPIPAS) Data Privacy

Protection Mark (DP Mark), and has strongly recommended public authorities to adhere to the Personal Data Protection Management and Audit Manual and Personal Data Protection Implement Manual.

Outsourcing by FSIs is strictly regulated in Taiwan. The Regulations for FIs were entirely redrafted a few years ago but the ones for IIs were not. Further guidance is expected in the near future. Outsourcing offshore is an area that the FSC is active in. FIs have been subject to fines for unauthorised offshore outsourcing, including using software that accesses offshore third-party servers for transaction verification, anti-fraud and anti-money laundering purposes.

B. Relevant Regulations[1]

Full Title	Abbreviated Title	Regulator	Citation/Reference[1]
Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation	Regulations	FSC	N/A
Personal Information Protection Act	PIPA	FSC	N/A
Enforcement Rules of Taiwan's Personal Information Protection Act	Enforcement Rules	FSC	N/A
Banking Act, Paragraph 3, Article 45-1	Banking Act	FSC	N/A
Directions for Operation Outsourcing by Insurance Enterprises	Directions	FSC	N/A
Regulations Governing Personal Information Safeguarding by the Non-Public Entities Appointed by the Financial Supervisory Commission	FSC PIPA Regulations	FSC	N/A

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	A compliance analysis must be carried out on the CSP to ensure that the CSP and its Cloud Services meet legal, regulatory, contractual and business requirements.	Article 4 of Regulations and Article 5 of Directions Article 8 of Enforcement Rules and FSC PIPA Regulations
Review, monitoring and control	The Cloud Contract must include rights for the FSI to monitor and supervise the CSP.	Articles 6-10 of Regulations and Articles 7-11 of Directions Article 8 of Enforcement Rules and FSC PIPA Regulations
Audit	The Cloud Contract must grant rights to audit, access, and inspection to the Regulator.	Article 10 of Regulations and Article 11 of Directions Article 22 of PIPA

1) Citations do not work the same way in Taiwan, therefore they are not included here. In practice, the Regulations referred to here would be cited by reference to their full title (as provided here).

Confidentiality and security	The Cloud Contract must address confidentiality of Data and the adoption of proper security measures. It is implied that the standard must be the same as that to which the FSI would be held.	Article 10 of Regulations and Article 11 of Directions Article 27, PIPA Article 12 Enforcement Rules and Article X of FSC PIPA Regulations
Resilience and business continuity	FSIs must establish risk management principles and operating procedures with CSPs. FIs that enter into an offshore outsourcing must ensure that they have a contingency plan and carry out a third-party assessment of the outsourcing plan if related to the outsourcing of Data entry, Data processing, and information systems.	Articles 4, 6-10 of Regulations. Articles 5, 7-11 of Directions Articles 18 and 19 of Regulations
Data location	There is no general prohibition (as long as the offshore outsourcing has been approved and complied with) on transferring Personal Data outside of Taiwan, provided that safeguards have been put in place (including contractual measures) to ensure that Personal Data is protected to a comparable standard of protection as it is under the PIPA. The authorities in Taiwan have the right to restrict the cross-border transfer of Personal Data. The only current prohibition is from the National Communications Commission that prohibits all Taiwanese telecommunications and broadcasting companies from transferring their Customer Data to the People's Republic of China. This prohibition is not relevant to FSIs.	Article 21 of PIPA Article 7 of Regulations and Article 8 of Directions
Data use	FSIs can only provide Data to CSPs that is necessary for the Cloud Services. CSPs must not use the FSIs' Data for any purposes other than that which is necessary to provide the Cloud Services. The Cloud Contract must include this protection for Data.	Articles 7 and 19 of the Regulations. Article 8 of Directions Article 10 of Regulations and Article 11 of Directions
Data segregation	The FSI's Data must be segregated from other Data held by the CSP. The CSP must be able to identify the FSI's Data at all times and be able to distinguish it from other Data held by the CSP.	Articles 10 and 19 of Regulations and Articles 8 and 11 of Directions
Subcontracting	The Cloud Contract must state that the CSP will not subcontract without the prior written consent of the FSI. The Cloud Contract must state scope, limitations, and conditions for subcontracting.	Article 10 of Regulations and Article 11 of Directions
Termination	The Cloud Contract must specify material events that would be cause for termination including termination under instruction of the Regulator.	Article 10 of Regulations and Article 11 of Directions

13. Thailand[1]

A. Overview

Is the use of Cloud Services permitted?	Yes.
Who are the relevant Regulators?	The Bank of Thailand (www.bot.or.th/English, ธนาคารแห่งประเทศไทย) ("**BOT**") regulates FSIs (except for insurance companies which are separately regulated in Thailand by the Ministry of Finance and Office of Insurance Commission (www.oic.or.th/en/home/, สำนักงานคณะกรรมการกำกับและส่งเสริม การประกอบธุรกิจประกันภัย(คปภ.)) ("**OIC**")). The OIC does not have any approval requirements for the use of Cloud Services. The OIC also has no specific requirements for IT outsourcing, but does set a minimum general requirement that insurance companies must have internal controls with regard to their IT service providers (including CSPs). This means that insurance companies have the latitude to develop their own internal controls, which the OIC in practice does not inspect or oversee. For the purposes of this jurisdiction, insurance companies are not discussed further.
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	Yes. According to the new IT Outsourcing Policy, Cloud Services or Cloud Computing is considered a "Critical IT Outsourcing", or in other words, very important services for the FSIs. For Cloud Services, the BOT specifically requires the FSI who wishes to use Cloud Services to consult with the BOT prior to engaging the Cloud Services. And since the use of Cloud Services is deem to be a Critical IT Outsourcing, it falls under "specific control" principle (Section 5.5.2 of the IT Outsourcing Policy) which requires 30 days advance notice to the BOT prior to the use of such services if the CSP is not an affiliate of the FSIs.

1) Prepared with assistance from Blumenthal Richter & Sumet (www.brslawyers.com).

According to the IT Outsourcing Policy and the Outsourcing Policy, there are three categories of activity: (i) material (activities that if disrupted would greatly impact the FSI); (ii) non-material (activities that support the operation of the FSI, including activities such as document storage); and (iii) low-risk (activities such as cleaning services).

Within material activities are two separate groups:

(a) "strategic functions" (which relate to decision-making aspects of the FSI's business and which may directly affect the capital, income or profit of the business), which cannot be outsourced at all, except the FSIs with business model which assemble the core of the work at the head quarter or certain specific branch for more efficiency which can apply for an approval from the BOT on a case by case basis; and

(b) "non-strategic functions" (functions not related to the strategy of the FSI but which support the strategy, such as finance and accounting), which can be outsourced without the BOT approval for the use of local outsourcing services. However, an approval is required if the outsourcing services come from outside of Thailand.

If activities are non-material, FSIs do not need to notify the BOT. However, FSIs are advised to consult with the BOT prior to making a decision as to materiality of the activities. This is because the BOT may disagree with the FSI's opinion regarding the materiality of the activities.

If activities are low-risk, no notification or approval requirement applies.

Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?

The Outsourcing Policy contains a very short form questionnaire for FSIs undertaking outsourcing. This is intended to help demonstrate compliance with the three significant issues that BOT considers FSIs must address. It is not a comprehensive questionnaire. The form does not need to be submitted where the outsourcing falls into the category of "low risk" or "non-material" but FSIs are advised to consult with BOT to ensure that the BOT is not of the view that the activities fall into the category of "material outsourcing". The form should be submitted by FSIs together with a letter of intent explaining its intention to outsource certain services.

	BOT states that FSIs are able to submit additional information if they wish and also free to adjust the method of presentation of the information (for example using diagrams etc.). All forms submitted to the BOT must be kept on file at the FSI as the BOT has authority to conduct on-site inspections of all activities of the FSI and its files. In addition, the IT Outsourcing Policy contains some additional notification requirements applicable to FSIs undertaking outsourcing in relation to IT services.
Are there specific contractual requirements that must be adopted?	Yes. BOT does mandate contractual requirements that must be agreed by FSIs with their CSPs. Principle 5 in Annex 3 of the Outsourcing Policy requires FSIs to enter into an agreement with outsource providers and specifies a minimum list of things that BOT would expect this to cover. In addition, Section 5.5.1 (3.2) of the IT Outsourcing Policy includes some additional contractual requirements that the BOT expects to be included for outsourcings involving IT services. The Cloud Contract must be in writing.
Other information/developments	There are currently no general Privacy Regulations in Thailand. A draft has been under consideration for a number of years but it is not known when this draft Privacy Regulation will come into force.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
IT Outsourcing Policy Sor Nor Sor 6/2557	IT Outsourcing Policy	BOT	Sor Nor Sor 6/2557
Outsourcing Policy Sor Nor Sor 8/2557	Outsourcing Policy	BOT	Sor Nor Sor 8/2557

C. Summary of the key requirements

Topic	Summary	Citation
Due diligence	FSIs must undertake a thorough due diligence of CSPs, including an assessment of: (a) technical capability, expertise and experience; (b) financial status; (c) business reputation; (d) records of complaints or litigations; (e) culture and expertise with FSIs; (f) capacity to adjust to change and develop; and (g) any risks of concentration.	Outsourcing Policy Principle 2 of Annex 3
Review, monitoring and control	FSIs must have a clear written outsourcing policy which must set out key issues such as the process for evaluation and managing risk, compliance with the laws of Thailand, any additional risk monitoring requirements and relevant internal control in place. The FSI must have provisions in its Cloud Contract that include internal control systems including performance reporting obligations, risk management, service standard and the steps for inspection and evaluation of the CSP's performance.	Outsourcing Policy Principle 1 of Annex 3 IT Outsourcing Policy Section 5.5.1 (3) Outsourcing Policy Principle 1 of Annex 3
Audit	FSIs must have provisions in their Cloud Contracts and outsourcing policy that allow the BOT, external auditors or other government agencies to inspect CSPs.	Outsourcing Policy Sections 5.6 and 5.7 IT Outsourcing Policy Section 5.7
Confidentiality and security	FSIs must make sure that CSPs have in place systems to ensure the security of the FSIs' Data. This must include strict designation of access rights and controls over staff.	Outsourcing Policy Principle 3 of Annex 3
Resilience and business continuity	FSIs must ensure that CSPs prepare a business continuity plan. FSIs must have in place a plan for covering emergencies and problems (including steps and methods for resolution of problems, indication of persons responsible and processes for revision and testing of the plan).	Outsourcing Policy Principle 3 of Annex 3 IT Outsourcing Policy Section 5.5.1(2)
Data location	BOT does not prohibit offshore outsourcing provided that the FSI must take into account any incidental risk factors including potential for change in political, foreign policy or law in the relevant countries and any additional risk monitoring requirements.	Outsourcing Policy Principle 6 and 7 of Annex 5 IT Outsourcing Policy Section 5.5.1(3.2)

Data use	FSIs must have provisions on security and confidentiality as well rights to access to and ownership of their Data in the Cloud Contract. The Cloud Contract must include sanctions in the event of disclosure of FSIs' Data. The Cloud Contract must also include arrangements regarding the method for receipt and transmission of Data and storage of Data.	Outsourcing Policy Principle 5(8) of Annex 3 IT Outsourcing Policy Section 5.5.1(3.2)
Data segregation	The FSI's Data must be separated from that of other customers of the CSP.	IT Outsourcing Policy Section 5.5.1(4) Outsourcing Policy Principle 3(1) of Annex 3
Subcontracting	The FSI must have provisions to ensure that, where the CSP uses a subcontractor, the subcontractor must comply with the key requirements for the Cloud Contract. The FSI must also clarify that responsibility for performance rests with the CSP. The FSI may choose to indicate in the Cloud Contract that the CSP must inform the FSI or obtain its permission before undertaking subcontracting or changing subcontractors.	Outsourcing Policy Principle 5(9) of Annex 3 Outsourcing Policy Section 5.6 IT Outsourcing Policy Section 5.2(1)
Termination	There must be provisions in the Cloud Contract for the FSI to take over the services or engage another CSP in the event of termination or change in CSP. Upon expiry or cancellation of the arrangement, Customer Data must be destroyed or returned by the CSP.	Outsourcing Policy Principle 3(5) of Annex 3 IT Outsourcing Policy Section 5.5.1 (3.2)

14. Vietnam[1]

A. Overview

Is the use of Cloud Services permitted?	Yes. In practice, a number Cloud Services are provided to Vietnamese FSIs by local and international CSPs.
Who are the relevant Regulators?	The State Bank of Vietnam (www.sbv.gov.vn, Ngân hàng Nhà nước Việt Nam) (**"SBV"**) regulates the use of information technology applications (including Cloud Services) in the financial services sector in Vietnam. The Ministry of Information and Communications (english.mic.gov.vn/Trang/default.aspx, Bộ Thông tin và Truyền thông) (**"MIC"**) regulates the telecoms and information technology sector in Vietnam.
Are there specific regulations dealing exclusively with Cloud Services?	No.
Are there other regulations/guidelines that are relevant?	Yes. See Section B.
Is regulatory approval required?	No. There is no requirement for approval. However, FSIs have to satisfy certain conditions to use Cloud Services provided by a third party and submit periodical reports on information security rules and operations to the SBV. The SBV is concerned in particular about the information security levels provided by the CSPs. In addition, foreign CSPs, which provide cross border Cloud Services to Vietnamese FSIs, have to have Vietnamese representatives domiciled in Vietnam in order to complete all statutory procedures in relation to taxes and fees payable in Vietnam. The MIC may issue regulations on cross border information technology services (but as yet has not done so). In principal, FSIs are entitled to engage CSPs at their discretion upon self-assessment and evaluation.

1) Prepared with assistance from Frasers Law Company (www.frasersvn.com).

Is there a process to follow? If so what is the process and is there a specific form/questionnaire to be completed?	No.
Are there specific contractual requirements that must be adopted?	Yes. The SBV sets out specific contractual requirements for information technology services providers (including Cloud Services)[1] as follows: • Cloud Contracts must address the liability of CSPs in relation to information security including but not limited to applicable penalties and indemnities if CSPs fail to ensure the information security which would adversely affect the confidentiality, availability, efficiency and recoverability of the information. • Cloud Contracts must include rights for FSIs to monitor and control access to Data held by the CSPs. • Cloud Contracts must include confidentiality obligations on CSPs (and these must be passed on to their personnel) and information security obligations.
Other information/developments	The Vietnamese Government has been publicly consulting on the Draft Decree for IT Services (which includes Cloud Services) since 2011. If the draft of the Decree is officially issued by the Vietnamese Government by the end of 2014 (as announced by the MIC), CSPs might be subject to operating licenses to be issued by the MIC. The information technology service provider community is working with the MIC to lobby for the removal of the requirement to obtain an operating license for Cloud Services. According to a limited survey (published on the SBV's website) in relation to Cloud Services, out of 31 FSIs surveyed in Vietnam, by the end of 2013, 6 were using Cloud Services and 25 had plans to implement Cloud Services by 2015.

1) Article 6 of Circular 1.

B. Relevant Regulations

Full Title	Abbreviated Title	Regulator	Citation/Reference
Law on Information Technology No.67/2006/QH11 passed by the National Assembly of Vietnam on 29 June 2006	IT Law	MIC	Law on Information Technology No.67/2006/QH11
Law on Credit Institutions passed by the National Assembly of Vietnam on 16 June 2010	Law on CI	SBV	Law on Credit Institutions
Law on the State Bank of Vietnam passed by the National Assembly of Vietnam on 16 June 2010	Law on SBV	SBV	Law on the State Bank
Circular 01/2011/TT-NHNN dated 21 February 2011 of the SBV on information security in the banking sector	Circular 01	SBV	Circular 01/2011/ TT-NHNN
Circular 29/2011/TT-NHNN dated 21 September 2011 providing information security in Internet banking services	Circular 29	SBV	Circular 29/2011/ TT-NHNN
Draft of Decree on Information Technology Services (updated on April 2014)	Draft Decree on IT Services	MIC	N/A

C. Summary of key requirements

Topic	Summary	Citation
Due diligence	FSIs must carry out a risk assessment and due diligence on CSPs to ensure that CSPs and the Cloud Services meet technical, financial and human resource requirements and capabilities and contractual and business requirements.	Article 6 of Circular 01
Review, monitoring and control	FSIs must be able to monitor and control CSPs, including by obtaining regular reporting and information, to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the Cloud Contract. FSIs must regularly review the reports and performance levels. The Cloud Contract must provide a mechanism for remedial actions for any issues that emerge.	Article 6 of Circular 01
Audit	The regulations do not require the Regulator to have a right to audit the CSP. However, FSIs must audit the CSP before entering into the service contract. There are no further requirements.	Circular 01
Confidentiality and security	FIs must adopt a sound and robust technology risk management framework and consider carefully the use of Cloud Services. CSPs must maintain robust security measures and comprehensive security policies. CSPs must use encryption technology to protect and secure the FSIs' Data at all times.	Article 6 and Article 10 of Circular 01
Resilience and business continuity	CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives. CSPs must regularly test and update procedures and systems in place to meet those objectives. The risk of downtime must be minimised through good planning and a high degree of system resilience.	Article 14 of Circular 01
Data location	There is no prohibition on FSIs on transferring Data outside of Vietnam. An FSI maymay transfer Data outside of Vietnam, provided that it has put in place safeguards (including contractual measures) to ensure that Data is protected to a comparable standard of protection [COMPARABLE TO VIETNAM?]. However, information which is considered a "national secret" may be subject to transfer restrictions or conditions. For example, certain information in relation to the	Circular 01

	deposits and other assets of Customers may considered to be national secrets. In practice, FSIs can obtain and have obtained; permits from the SBV to transfer this information outside of Vietnam.	
Data use	CSPs must not use FSIs' Data for any purpose other than that which is necessary to provide the Cloud Services. The Cloud Contract must prevent CSPs from using FSI Data for any secondary purpose at all times.	Law on CI
Data segregation	The Cloud Contract must provide for data segregation.	Article 6 Circular 01
Subcontracting	The Cloud Contract must provide for subcontracting by CSPs.	Article 6 of Circular 01
Termination	The Cloud Contract must provide for termination of the contract.	Article 6 of Circular 01

Part 6: Quick Reference Glossary

"Cloud Contract" means the contract between the FSI and the CSP for the provision of Cloud Services, such as an outsourcing services agreement which includes the provision of Cloud Services.

"Cloud Services" means on-demand network access to a shared pool of configurable computing resources. Cloud Services provide FSIs 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 FSI. In this report, the Cloud Services generally referred to are Public Cloud Services.

"Community Cloud Services" are Cloud Services that serve members of a community of customers with similar computing needs or requirements, such as security, reliability and resiliency. The infrastructure may be owned and managed by members of the community or by a CSP. The infrastructure is located either on customer premises or the CSP's premises. Community Cloud Services are a 'multi-tenanted solution' because there are multiple members of a community of customers who will all have access to the same infrastructure.

"CSP" means cloud service provider, i.e. a third party that provides Cloud Services.

"Customer" means a customer of an FSI, such customer may be an individual, a company, an organisation or another FSI.

"Customer Data" means any Data which relates to Customers of the FSI. It is a subcategory of Data. Customer Data, may be defined differently from jurisdiction to jurisdiction.

"Data" may include the FSI's business confidential information, information about the FSI's Customers, Personal Data relating to the FSI's Customers and/or the FSI's staff. When using Cloud Services, FSIs may transfer various kinds of data to CSPs, for CSPs to help store, manage and/or process. There are two key subcategories of Data: Customer Data and Personal Data.

"DC" means a data centre used to host Data as part of the provision of Cloud Services.

"FSI" means financial services institution, including banks and insurance companies.

"Financial Regulator" means a regulatory body with supervisory authority over FSIs.

"Hybrid Cloud Services" are Cloud Services that are combination of Private Cloud and Public 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 Public Cloud). Hybrid Cloud Services may be a 'multi-tenanted solution', if multiple customers have access to the same infrastructure. It can however also provide a 'dedicated' solution or component.

"ISO/IEC 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.

"ISO/IEC 27002" is a set of guidelines published by the International Organization for Standardization that provides for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

"ISO/IEC 27018" is a set of guidelines published by the International Organization for Standardization that specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of Personal Data which might be applicable within the context of the information security risk environment(s) of a provider of Public Cloud Services.

"Personal Data" is a subcategory of Data. Personal Data (or similar terms in Privacy Regulations) may be defined differently from jurisdiction to jurisdiction. For the purposes of this report, it means broadly any data that relates to an individual, including personally identifying information or information associated with or derived from an individual's use of the FSI's financial services or as a result of the relationship as a Customer of or member of staff of the FSI.

"Privacy Regulations" means Regulations that govern the FSIs collection, use and disclosure of Personal Data.

"Private Cloud Services" are Cloud Services in which the infrastructure is owned 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 infrastructure from which the Data and Cloud Services are provisioned is for the exclusive use of a particular customer.

"Public Cloud Services" are Cloud Services in which the infrastructure being used is owned and managed by the CSP and is located off-premise from the FSI. Although the Data and services are protected from unauthorised access, the infrastructure is accessible by a number of different customers of the CSP. Public Cloud Services are also referred to as a 'multi-tenanted solution' because there are multiple customers who will all have access to the same infrastructure.

"Regulations" means laws, regulations and regulatory guidelines which govern the use of Cloud Services by FSIs. This term is used to refer to Regulations published by Financial Regulators, e.g. regulations on outsourcing, technology, business continuity etc.. In many jurisdictions covered by this report, although a Regulation may be called or referred to as a guideline, such guidelines are still expected by Regulators to be (and are in practice) complied with.

"Regulator" means a Financial Regulator or a Privacy Regulator.

asia cloud computing association

About the Asia Cloud Computing Association (ACCA)

The ACCA is an industry association that represents stakeholders of the cloud computing ecosystem in Asia. Our mission is to accelerate the adoption of cloud computing through Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services. Through dialogue, training, and public education, the ACCA provides a vendor-neutral platform to discuss strategies, share ideas, and establish policies and best practices relating to cloud computing.

For more information on the ACCA, membership and partnership opportunities, visit http://www.asiacloudcomputing.org, email info@asiacloudcomputing.org, tweet us @accacloud, or join our LinkedIn group http://is.gd/accacloud