Asia's Financial Services on the Cloud 2018

Regulatory Landscape Impacting the Use of Cloud by Financial Services Institutions in Asia

Acknowledgments

The ACCA would like to acknowledge the Members of the Financial Services Industry Special Interest Group (FSI SIG) for their contributions:

Sassoon Grigorian, Salesforce (Chair)
Quint Simon, AWS
Roger Somerville, AWS
Brandon Lim, AWS
Amanpriet Dhingra, Equinix
Mary McHale, Equinix
Aruna Withane, Google
Andrew Kim, Google
Andrew Cooke, Microsoft
Joy Fuyuno, Microsoft
Stacy Baird, Chair of Working Groups

ACCA Secretariat:
Lim May-Ann, Executive Director
Cheryl Tan, Research Report Lead
Sagarika Senapaty, Director of Partnerships

About the Asia Cloud Computing Association:
The Asia Cloud Computing Association (ACCA) is a leading industry association comprising the stakeholders of the cloud computing ecosystem in Asia. The ACCA works to ensure that the interests of the cloud computing community are effectively represented in the public policy debate. Our primary mission is to accelerate the growth of the cloud market in Asia Pacific, where we promote the growth and development of cloud computing through dialogue, training, and public education. Through regular meetings, we also provide a platform for members to discuss implementation and growth strategies, share ideas, and establish policies and best practices relating to the cloud computing ecosystem.

Asia's Financial Services on the Cloud 2018

Regulatory Landscape Impacting the Use of Cloud by Financial Services Institutions in Asia

Contents

FOREWORD

Over the last few years, we have seen the rapid acceleration of cloud adoption in the financial services sector.

In a globally competitive environment, the financial services sector is continually building upon improving customer service in a safe and secure environment.

Since this report was published in 2015, we have seen updates in outsourcing guidelines among Financial Regulators across the region. There have also been developments in technology whether it be blockchain, fintech or other financial service developments.

There is an improved understanding of cloud services from regulators, and more nuanced outsourcing guidelines, which by-and-large has led to an uptake of services from the financial services sector.

But as always, there is more to do.

This report provides an update of jurisdictions which have updated their guidelines since 2015, and provides clear concise recommendations for regulators.

It is imperative that regulations should start to work towards a consistent definition of outsourcing between jurisdictions. Definitions of outsourcing vary from country to country. This should be consistent across the region to ensure efficient use of services as well as to reduce compliance requirements.

There also needs to be a clear distinction of services deemed material or critical to FSIs, and those deemed non-critical.

Banks and the financial services sector have been using cloud computing for years in areas such as web content management and customer relationship management software.

Some institutions are looking towards moving core systems to the cloud to offer greater flexibility, and efficiency.

This will be a challenge or opportunity for regulators and cloud service providers for the decade to come.

Special acknowledgement to the ACCA Secretariat for developing this report with my FSI Special Interest Group colleagues representing AWS, Equinix, Microsoft, and Google.

Sassoon Grigorian
Chair of the ACCA Financial Services Industry Special Interest Group, and Head of Public Policy, ANZ & SE Asia, Salesforce

EXECUTIVE SUMMARY

A Report on the Regulatory Landscape Impacting the Use of Cloud by Financial Services Institutions in Asia

1. Asia Pacific (APAC)'s Financial Services Institutions (FSIs) are rapidly digitising their processes using cloud and new technology. This has allowed them to become more cost-efficient, as they streamline business processes.
2. Cloud computing has also been shaping the way FSIs respond to new consumer habits, evolve to meet the needs of a new competitive landscape, and adjust to heightened compliance requirements.
3. A laggard in this is the migration of core FSI systems to public cloud; this area remains an untapped potential for efficiency gains. The ACCA expects to see more changes in these systems in the coming years as pressure to innovate and costs of upgrading legacy core systems increase.
4. FSIs have increasingly integrated technology into their day-to-day operations. The regulatory landscape has evolved to meet this trend, with the creation of fintech regulatory sandboxes and national payment gateways, support for open banking protocols, and implementation of mandatory data breach reporting regimes.
5. Regulators play a crucial role in enabling – or impeding – the growth of Cloud Services. While some APAC Regulators are clarifying outsourcing rules and guidelines to help firms achieve compliance, regulatory restrictions and cloud adoption blockers still exist.
6. This report identifies where and how regulations currently allow FSIs to adopt Cloud Services and where there is room to improve the current regional regulatory landscape, and makes recommendations to help Regulators break down some remaining barriers. The ACCA's seven key recommendations are:
    - Regulations should be **technologically neutral**. There should not be separate regulations for the use of Cloud Services.
    - Regulations should set out a **clear process** for FSIs to follow when adopting Cloud Services, where the use of Cloud Services **should not require regulatory approval**.
    - Regulations should have a **clear distinction of services deemed material or critical to FSIs**, and those deemed non-critical.
    - Regulations should have a **clear distinction between control vs possession of data**, and distinguish the roles and responsibilities for controls of an FSI's data accordingly.
    - Regulations should **permit the transfer of Data to other jurisdictions** without requiring Data localization, subject to appropriate safeguards (e.g. security, business continuity, access, and audit).
    - Regulations should only identify the key issues that should be addressed in Cloud Contracts. They **should not be prescriptive** of the terms of Cloud Contracts.
    - Regulations **should not require unrestricted audit access rights** to FSIs and regulators. Independent third-party audits should be an allowed option for verifying a cloud service provider (CSP)'s physical security controls.

1. REGIONAL REGULATORY UPDATE 2018: ASIA'S FINANCIAL SERVICES INDUSTRY

Since the ACCA last published its financial services report in 2015, Asia-Pacific (APAC)'s financial services sector has dialled up its use of technology. From decisions on using cloud computing to enabling innovation in fintech such as through e-wallets, m-payments, and the use of blockchain – the pace of tech adoption in APAC's financial services sector is nothing short of breathless. The ACCA noted these trending developments in 2015, and released a summary report charting the regulatory conditions impacting the use of Cloud Services by APAC's financial services institutions (FSIs).

a. Report Summary – About the 2018 Asia's Financial Services on the Cloud Report

This report updates our 2015 research on the regulatory landscape impacting Cloud Services in APAC. It updates the current approaches governments and Regulators in nine selected APAC markets have taken towards cloud computing, and the environment these relevant policies and regulations have created for cloud adoption in the financial services sector.

Financial Regulators' **outsourcing guidelines** have a key role to play in shaping this environment, and can determine the extent FSIs can benefit from cloud computing technology. As with the previous report, we provide an overview of the regulatory landscape in **Part 1.** of this report. We also review and elaborate on best practice examples of the ten key cloud outsourcing risk management requirements that must be addressed in order for an FSI to adopt Cloud Services: 1. Due Diligence Process for Cloud Adoption, 2. Review, Monitoring and Control, 3. Audit, 4. Confidentiality and Security, 5. Resilience, Business Continuity and Disaster Recovery, 6. Data Transfer and Location, 7. Data Use Limitations, 8. Data Segregation, 9. Cloud Contracts and Subcontracting, and 10. Exit and Termination. This is followed by **Part 2.** which summarises the relevant regulations in each market according to these requirements.

b. Trends in Cloud Adoption in the Financial Services Sector

i. Cost and Security Drivers Behind Rising Cloud Adoption

Cloud Services offer FSIs cost-efficiency to deal with the rising cyber security threats and competition from the burgeoning fintech sector. Besides economies of scale from using shared Cloud Services, FSIs on cloud computing receive a competitive advantage over those in their industry that do not: Cloud Service Providers (CSPs) can provide the most up-to-date security 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. This report illustrates some of these benefits through a number of case studies.

ii. More Established Use Cases for FSI on Cloud

FSIs have started outsourcing the processing of Data that requires significant computing resources. This includes tasks that may involve Customer Data or Personal Data such as running high volumes of complex analytics calculations to evaluate clients' risk profiles and run business model simulations. FSIs are also using Cloud Services to run system sandboxes to test system updates or changes without the risk of affecting the rest of their operations.

iii. Untapped Potential in the Migration of Core Systems to the Cloud

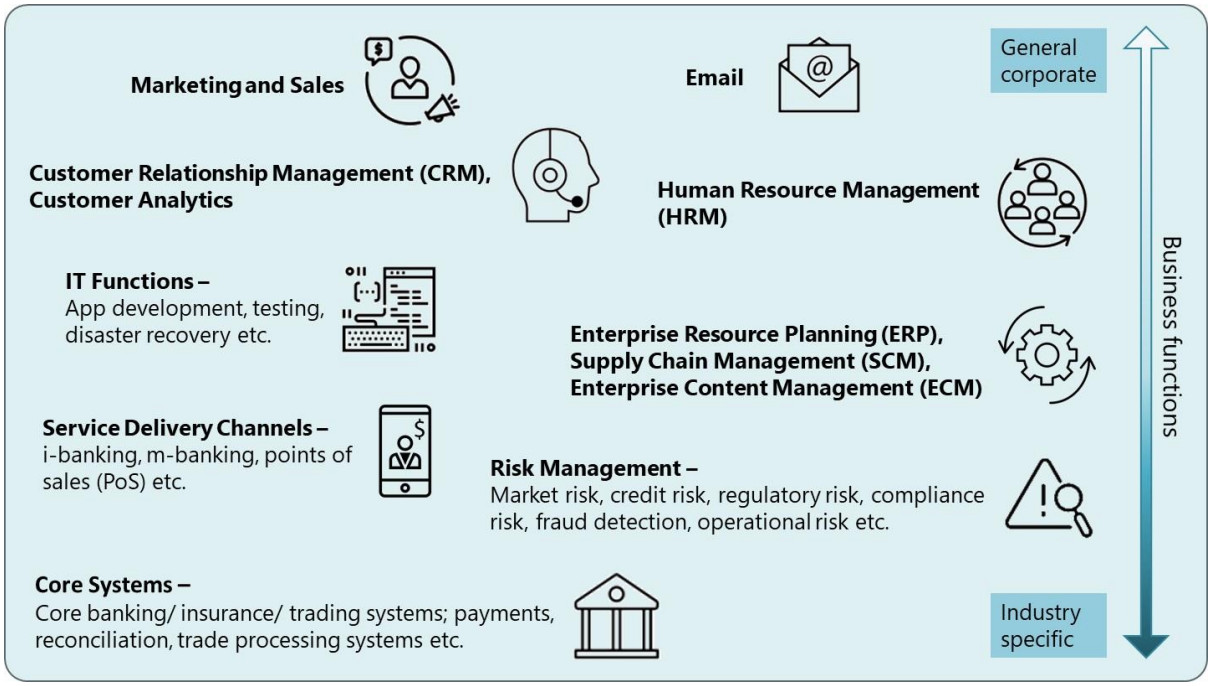
As cloud computing consistently proves its worth following its deployment in various organisational functions in the financial sector, the migration of core systems to the cloud will be the next frontier of cloud adoption in the financial services sector in 2018 and beyond. As the pressure to innovate increases, and costs of upgrading legacy core systems rise accordingly to support this, FSIs are considering shifting their core systems – which typically take up the bulk of their IT budgets – to the public cloud. A 2016 study by Temenos revealed that the proportion of banks running mission-critical applications, including core processing, on the cloud rose to 3% from

1% in 2015.[1] While this figure is still relatively modest, Regulators' recognition of the suitability of cloud adoption and the availability of case studies of FSIs that have successfully shifted their core processes to the cloud are credited as impetus for the gradual perception shift. As the cost of *not* migrating to the cloud increases, we anticipate this trend to gain further traction over the next few years.

iv. Case Studies of Successful Cloud Adoption

Successful adoption of Cloud Services has been illustrated in this report through a number of case studies, where FSIs have been able to leverage cloud-based capabilities to transform their business functions. Some of the key benefits driving FSIs' adoption of Cloud Services include the ability to generate cost savings, streamline internal business processes, enhance customer service delivery and accelerate product innovation.

Figure 1 – Financial Services Business Functions' Digital Transformation Through Cloud



Source: Asia Cloud Computing Association, 2018

[1] https://www.temenos.com/globalassets/mi/rep/9th_annual_temenos_survey-open_for_business-wo-f.pdf

Case Study:

Financial Services and Relationship Analytics

For the traditional financial services sector, embracing digital technologies alone has not been enough to drive productivity, efficiency and business growth. A new generation of cloud-based analytics provides FSIs with the ability to gain new insights from organisational relationship data to measure customer engagement, improve processes and identify risks early.

Leveraging relationship networks for sustainable long-term returns means that it is critical to break down internal silos – a much greater challenge to legacy FSIs than their newly emerging fintech rivals. Relationship analytics is giving a new impetus to FSIs to improve customer intelligence, risk and regulatory management and growth by understanding the value creation networks that operate across the organisation.

Risk and regulatory management

Fraud continues to dominate FSI agendas, and rising compliance demands and regulatory scrutiny are forcing FSIs to re-evaluate their efforts. New generation analytics are emerging as key tools to improve fraud and criminal activity detection. For example, data analytics detects potential internal fraud by examining employees' communication lines and alerting investigators of atypical patterns that may signal collusion between employees. This prevention mechanism enables FSIs to identify and manage potential threats before they materialise, increasing the effectiveness of an FSI's compliance and vigilance activities and minimising the financial, legal or reputational damage that internal fraud may cause.

Cloud computing further enhances the power of data analytics by overcoming the storage limitations of on-premise servers, allowing FSIs to gain greater data-driven insights. With trusted cloud partners, data can be processed and aggregated in real time as part of an FSI's anti-money laundering (AML) and know your customer (KYC) processes. This automation enables data to be pieced together to discover new money laundering patterns, which may be easily overlooked when the processes are divided and conducted manually across large compliance teams.

Customer experience and sales processes

Recently, APAC FSIs have begun expanding digital platforms to front-facing departments to create a better customer experience, improve sales processes and for account management. By identifying organisation-wide relationship and customer interactions, including those not in customer relationship management (CRM) systems, frontline and sales employees can get a holistic view of their customers. These automatically-generated, real-time insights give executives an understanding of sales teams' customer interactions, and enable them to make better-informed decisions in managing staff activity, improving productivity and efficiency.

Evidence-based human resources

To create a sustainable internal advantage, FSIs are also extending digital transformation to benefit the people whose data is being analysed. Diverse workplace networks offer rich insights into actual workflows for more meaningful data-driven decisions by Human Resources and management. Network patterns across an organisation generate insights that quantify the impact of leaders on their team, recognise line manager effectiveness, identify high potential employees (HIPOs), improve succession planning and detect signs of employee burnout.

APAC FSIs have already implemented pilot initiatives positioning the region as a potential leader in the adoption of Relationship Analytics. One such APAC FSI applied relationship analytics to its leadership program to validate chosen candidates and identify potential candidates that may have been overlooked. FSIs in emerging markets within APAC are a particular bright spot, as they are able to dive straight into next-gen technologies while avoiding sunk costs in legacy IT infrastructure.

Source: Thanks to TrustSphere for providing this case study. For more info, contact marketing@trustsphere.com or visit https://www.trustsphere.com/

c. State of FSI Cloud: Regulatory Recommendations[2]

The ACCA has seven policy recommendations to Regulators, which would improve the conditions for FSIs' adoption of Cloud Services:

1. Regulations should be **technologically neutral**. There should not be separate regulations for the use of Cloud Services.

2. Regulations should set out a **clear process** for FSIs to follow when adopting Cloud Services, where the use of Cloud Services **should not require regulatory approval**.

3. Regulations should have a **clear distinction of services deemed material or critical to FSIs**, and those deemed non-critical.
   - This is important for FSIs when considering the risk management framework it should adopt for each of its outsourcing arrangements, and can be addressed through "Whitelists".

4. Regulations should have a **clear distinction between control vs possession of data**, and distinguish the roles and responsibilities for controls of an FSI's data accordingly.
   - As CSPs share the responsibility for owning and controlling data with their customers in a model of shared responsibility, the control of data needs to be recognised as a distinct concept from possession of data as it revolves around the ability of a party (the data controller) to exercise stewardship over data, to be confident that the data is up-to-date, and to access or recover that data in the event that the primary data repository is not available for any reason.

5. Regulations should **permit the transfer of Data to other jurisdictions** without requiring a local copy, subject to appropriate safeguards (e.g. security, business continuity, access, and audit).

6. Regulations should only identify the key issues that should be addressed in Cloud Contracts. They **should not be prescriptive** of the terms of Cloud Contracts.

7. Regulations **should not require unrestricted audit access rights** to FSIs and Regulators. Independent third-party audits should be an allowed option for verifying a CSP's physical security controls.
   - CSPs may operate in a multi-tenant public cloud or a Software-as-a-Service (SaaS) business model, and may not be able to provide customers with unimpeded access to their premises and systems. In these instances, FSIs or regulators are able to extract customers' specific logs, data etc. through an audit process that does not involve access to a CSP's physical premise.

The recommendations table below compares these key recommendations across the regulations in nine APAC jurisdictions, showing the status of implementation of these recommendations as of the date of publication of this report.

[2] Recommendations 1, 2, 5, 6, and 7 were originally in the 2015 report, and where relevant, have been revised for this edition. Recommendations 3 and 4 are new to the 2018 recommendations.

Table 1 – Assessment of APAC Markets Against the ACCA's Cloud Regulation Recommendations for the Financial Services Sector

Recommendations	Australia	Hong Kong	India	Indonesia	Malaysia	New Zealand	Philippines	Singapore	South Korea
1. Regulations should be **technologically neutral**. There should not be separate regulations for the use of Cloud Services.									
2. Regulations should set out a **clear process** for FSIs to follow when adopting Cloud Services, and use of Cloud Services **should not require regulatory approval**.									
3. Regulations should have a **clear distinction of services deemed material or critical to FSIs**, and those deemed non-critical.									
4. Regulations should have a **clear distinction between control vs possession of data**, and distinguish the roles and responsibilities for controls of an FSI's data accordingly.									
5. Regulations should **permit the transfer of Data to other jurisdictions** without requiring a local copy, subject to appropriate safeguards (e.g. security, business continuity, access, and audit).									
6. Regulations should only identify the key issues that should be addressed in Cloud Contracts. They **should not be prescriptive** of the terms of Cloud Contracts.									
7. Regulations **should not require unrestricted audit access rights** to FSIs and regulators. Independent third-party audits should be allowed for verifying a CSP's physical security controls									

Recommendation implemented

Recommendation not implemented

Source: Asia Cloud Computing Association, 2018

Since 2015, several markets have adopted regulatory positions in line with this paper's five key recommendations. Namely, **Hong Kong, the Philippines**, **South Korea** and **Singapore**, have all made some progress in this respect. However, more needs to be done to completely remove cloud adoption blockers, as can be seen from the table above.

We also note that a number of APAC Regulators have moved towards clarifying rules and guidelines to aid firms in achieving compliance in their outsourcing activities.

- **Hong Kong**'s Privacy Regulator issued guidance on data privacy in the cloud in July 2015.[3]
- **New Zealand**'s central bank revised its outsourcing policy in February 2017,[4] reducing regulatory ambiguity by introducing a formal definition of outsourcing.
- **The Philippines'** central bank amended its outsourcing guidelines[5] to clarify that the FSI remains responsible for ensuring that its legal obligations are fulfilled through any

[3] https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf
[4] https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Policy-development/Banks/Outsourcing-policy-for-registered-banks/Completed/2017%2009%2019%20-%20Final%20BS11%20redraft_2.pdf?la=en
[5] http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf

outsourcing arrangements. However, restrictions to the use of outsourcing remain a barrier to cloud adoption by Philippines FSIs.

- **Singapore**'s central bank revised its outsourcing guidelines[6] to provide clarity on FSIs' compliance obligations while using Cloud Services in July 2016, at the same time removing administrative obligations that had to be met before FSIs could outsource certain business functions.
- **South Korea**'s Financial Regulators revised outsourcing regulations in June 2015[7] with an aim to relax conditions placed on FSIs when outsourcing their IT and data processing services. This however, only applies to less-significant information processing systems, which excludes the use of cloud for systems handling unique identification information and personal credit information, thereby restricting the FSIs' adoption of cloud.

While no markets covered by this update have subsequently regressed from their positions in 2015, regulatory restrictions and cloud adoption blockers continue to persist in APAC markets.

- For example, whilst **South Korea** has seen improved regulatory conditions that permit the use of cloud by FSIs, Regulators still require that FSIs first seek approval before using Cloud Services, and that personally-identifiable information is stored within the country.
- Data localisation continues to be a significant issue in **Indonesia**; further regulation has been passed mandating that firms keep disaster recovery resources within Indonesian borders, and firms must process personal and transaction data within Indonesia.
- This is also true in **Malaysia**, whose new Draft Outsourcing Guidelines and Interoperable Credit Transfer Framework (ICTF) have data localisation requirements. Furthermore, our assessment that Asia's markets have generally progressed in terms of cloud-friendliness may change with the implementation of these guidelines which, if finalised in its current draft form, could inadvertently reduce security conditions for Cloud Services by proposing to give FSIs and auditors the rights to access a CSP's premise, and limit scalability by stipulating maximum periods for outsourcing agreements.
- Most recently, **India** has taken a step in this direction through its Statement on Developmental and Regulatory Policies. All payment service operators, as well as their service providers and third-party vendors, are required to store their payments data within India by 5 October 2018 for the regulator's unrestricted access.

d. Emerging Regulatory Issues

i. Establishment of Fintech Regulatory Sandboxes

A number of Regulators have established fintech regulatory sandboxes which enable FSIs to develop and test out new products and services that use innovative technologies, such as cloud computing, within a controlled regulatory environment. **Malaysia**[8] and **Singapore**[9] launched their regulatory sandbox frameworks in 2016, while **South Korea**[10] established its sandbox in 2017, and **Indonesia** created a sandbox for payments systems operators[11] in 2017.

---

[6] http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf
[7] https://www.fsc.go.kr/downManager?bbsid=BBS0048&no=97044
[8] http://www.bnm.gov.my/index.php?ch=57&pg=137&ac=533&bb=file
[9] http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf
[10] http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=&sword=&r_url=&menu=7210100&no=32152
[11] http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/PADG_191417.aspx

Some markets have gone a step further to evaluate their existing sandbox regimes and refine them. For example, **Australia** has taken measures that address obstacles users have faced by expanding the testing timeframe and range of fintech products and services.[12] **Hong Kong** has also worked to break down barriers to innovation by connecting Financial Regulators' sandboxes and opening participation to non-FSIs.[13]

ii. Support for Open Banking Protocols

Open Application Programming Interface (API) and data-sharing initiatives are being adopted to create an environment where traditionally bank-captured data and proprietary algorithms are made available to both FSI and non-FSI financial services providers, with the aim of fostering competition and innovation in the broader financial services sector. For example, **Singapore**'s Privacy Regulator has approved a proposal[14] for organisations to share data for the purposes of fraud detection and abuse prevention without first receiving customers' consent and **Australia**'s open banking regime will allow FSIs' customers to own their data, and decide if they want to share that data with other banks, institutions or fintech companies.[15] **Hong Kong** has also consulted on its approach to an open API framework that would enable system and service integration between banks and other sectors including healthcare and retail, while encouraging transparency in the banking sector.[16]

Open banking protocols will require large amounts of data to be made available and shared between banks and other third parties. This runs the risk of data-sharing platforms being compromised and thus increases the need for stronger privacy protection and security measures. Cloud providers should take note of this development because of the opportunity for cloud-based solutions to address these security concerns. For example, large data sets can be stored and analysed securely on a single platform hosted on the public cloud, allowing for data sets to be accessed by FSIs, fintech companies and other stakeholders without the need for FSIs to invest in extra infrastructure to meet these additional regulatory obligations.

iii. Creation of National Payment Gateways

The formation of national payment gateways has emerged in **Indonesia**[17], **Malaysia**[18], **Thailand**[19] and **Vietnam** [20] with the intention of accelerating e-payment adoption by increasing the affordability of and access to electronic transactions. In considering the large amount of personal data that would be passing through these networks, data localisation has again emerged as a quick fix as policy makers deliberate the issue of data security.

Creating a centralised system that processes and stores all transaction data may create a "honey pot" that hackers and other cybercriminals will find difficult to resist. However, imposing a data onshoring requirement does not ensure that the system and its data are protected by the most robust security controls and measures. In fact, a data localisation requirement could instead result in data being less secure and at greater risk of loss, theft or unauthorised access than if it was stored with a competent CSP.

iv. Implementation of Mandatory Data Breach Reporting Regimes

Regulators are under considerable pressure to act on pressing issues such as cyber security and privacy, and their reaction to these issues may influence FSIs' use of Cloud Services. Mandatory

[12] https://treasury.gov.au/consultation/c2017-t230052/
[13] http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml
[14] https://www.pdpc.gov.sg/pdpc/news/latest-updates/2018/02/pdpcs-response-to-public-consultation-on-approaches-to-managing-personal-data-in-the-digital-economy
[15] https://treasury.gov.au/review/review-into-open-banking-in-australia/
[16] http://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180111-3.shtml
[17] http://www.bi.go.id/id/ruang-media/siaran-pers/Pages/sp_194917.aspx
[18] http://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement&ac=594
[19] http://www.bangkokbank.com/BangkokBank/PersonalBanking/SpecialServices/NationalEpayment/Pages/knowepayment.aspx
[20] http://napas.com.vn

data breach reporting laws have started to be mooted across the APAC region. **Australia**[21] has taken the lead on this front, with regulation which came into effect on 22 February 2018, with **Singapore**[22] following suit. **New Zealand**[23] and **India**[24] have shown similar interest in adopting such measures, and any high-profile data breaches in coming years will put increasing pressure on Regulators to enact similar laws. This will especially impact FSIs, which often store highly sensitive personal data of clients, and possibly their CSPs.

Mandatory data breach reporting laws stand to increase the administrative burden for organisations as data breaches have to be reported to both financial and privacy regulators under multiple legal regimes without enhancing the protection of individuals. This becomes a concern for CSPs when a clear distinction between a data controller and a data processor is not made, and responsibilities for each party to comply with the law is unclear. For example, FSIs, as data controllers, maintain control of personal data when using a Cloud Service, and in turn for data breaches and notifying affected individuals and the relevant regulators. On the other hand, data processors which are contractually limited from accessing data to the extent necessary to identify a breach, such as CSPs, should not be held liable to notify a data controller of a breach.

Part 2. of this report goes into further detail describing different policies and regulatory approaches taken by governments and Regulators in the nine APAC markets, and the environment these have created for cloud adoption in the financial services sector. For example, Financial Regulators that have adopted technology-neutral outsourcing and/ or technology risk management (TRM) guidelines to recognise cloud procurement as similar to any other type of outsourcing are generally perceived as more supportive of cloud adoption than those that have not.

[21] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
[22] https://www.pdpc.gov.sg/pdpc/news/latest-updates/2018/02/pdpcs-response-to-public-consultation-on-approaches-to-managing-personal-data-in-the-digital-economy
[23] https://www.resaeller.co.nz/article/633181/data-breach-notification-expected-become-mandatory-nz/
[24] http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited

Case Study:

Thailand's Siam Commercial Bank

Siam Commercial Bank (SCB) is Thailand's second-largest bank by total assets. In 1997, the Asian Economic Crisis gave many banks the impetus needed to overhaul their internal processes, in order to develop business models that would be capable of weathering a negative economy. This led SCB to embark on an innovation program that places its customers first, which in turn informed the decision to integrate Salesforce's Customer Relationship Management (CRM) cloud solutions into its key business operations.

The results have been phenomenal. SCB, which had built its asset portfolio up to a value of USD34 billion in its first one hundred years of business, saw this amount double to USD70 billion in just seven years. The bank attributes this success largely to its cloud-enabled ability to change rapidly to meet customers' evolving needs. This ability was complemented by a shift in internal company culture stemming from the implementation of cloud solutions, which saw once-cautious employees now hungry for change.

Gaining deep customer insight and lifting service levels

Putting customers first involves knowing them, and SCB leverages the Sales Cloud software to access deep insights into customers' needs. By doing so, SCB has been able to deliver solutions and packages that are tailor-made for people's individual lifestyles. For example, mobile- and Internet-based applications have been developed in response to customers' demands to be connected with banking services from anywhere, at any time.

SCB also has more than 10,000 service employees who are dedicated to providing a cloud-enabled customer experience. By using Service Cloud, the bank has been able to deliver consistent and high-quality service to its customers: in less than a minute from entering a branch, service employees are able to understand a customer's needs and engage him or her in meaningful conversation.

Source: Thanks to Salesforce for providing this case study. For more information, visit https://www.salesforce.com/au/customer-success-stories/scb/

e. Ten Key Cloud Outsourcing Requirements[25]

This section covers ten key requirements which we believe Regulators should address and provide clarity on, to ensure Cloud Services may be adopted by the financial sector.

1. Due Diligence Process for Cloud Adoption

While the processes for adopting Cloud Services and the regulations that apply differ from one jurisdiction to the next, there are many common themes including a minimum requirement for 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 checklists for any IT outsourcing by an FSI.

2. Review, Monitoring and Control

Compliance does not end when the outsourcing contract that includes Cloud Services is signed. Instead, Regulators require that the FSI continue to be vigilant in compliance throughout the Cloud Contract lifecycle. The FSI is usually 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.

3. Audit

Many regulations require audit rights, either for the FSI (sometimes recognising that this audit can be carried out by a third party), the Regulator or both. Ambiguity surrounding the scope, frequency and other details around audit rights, however, can cause difficulties when these rights are being negotiated. First, because oftentimes 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. As CSPs could be employing a SaaS business model and/ or operating in a multi-tenanted environment, granting FSIs or regulators wide-ranging audit rights could undermine the confidentiality and security policies that the CSP upholds.

4. Confidentiality and Security

Regulators understandably place a lot of emphasis on confidentiality and security, since this will protect an FSI's reputation and maintain high levels of customer confidence. Regulators require the FSI to ensure that the CSP maintains robust security measures and comprehensive security policies. FSIs should not, and will not, use Cloud Services if they are not secure. In addition, Privacy Regulators also require FSIs to maintain high levels of security in respect of Personal Data in order to ensure that the privacy of individuals is safeguarded and Personal Data does not get into the wrong hands.

5. Resilience, Business Continuity and Disaster Recovery

Cloud Services must be reliable. As a minimum, 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. Any service disruption to the FSI's operations can have significant impact on the stability of a country's financial system, and the wider community. Regulators recognise that service disruptions can happen but require that the risks of downtime are minimised through effective and appropriate planning and procedures and a high degree of system resilience.

6. Data Transfer and Location

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 allowed to be transferred to other jurisdictions. Regulators who are concerned about the transfer of Data

[25] More details of each of these may be found in the ACCA's 2015 report at http://www.asiacloudcomputing.org/research/2015-research/fsi2015

to other jurisdictions may want to ensure that the protection offered to the Data does not weaken when the Data leaves their jurisdiction, through security standards and encryption, such as international standard ISO/IEC 27017 detailing cloud security controls, and ISO/IEC 27018 detailing protection of personally-identifiable information in public cloud processors, and Payment Card Industry Data Security Standard (PCI DSS) which is an information security standard for credit card transfers.

7. Data Use Limitations

Regulators typically require FSIs to 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. 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.

8. Data Segregation

In many jurisdictions (such as South Korea), 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. This requirement helps to ensure that:

- Security and confidentiality of Data is maintained;
- The integrity of Data is preserved; and
- Termination of the Cloud Contract is easier to deal with since all the FSI's Data can be more easily returned and deleted.

9. Cloud Contracts and Subcontracting

It is good business practice for an FSI to enter into a Cloud Contract, which is 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. Regulations which lack detail in addressing this may lead to FSIs not being entirely sure what they should include in their Cloud Contracts, while 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, too much detail can also slow down the negotiation process and lead to disagreement between the parties because of differing understanding or interpretation of regulations.

For example, the general requirement that CSPs should be responsible for their use of subcontractors should be a term in the Cloud Contract, but finer details and conditions on the use of subcontractors should be negotiated between the FSI and CSP. Most CSPs will rely on the use of subcontractors to provide certain support services. This should not be a problem so long as subcontractors are subject to equivalent controls as the CSP.

10. Exit and Termination

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. The FSI must also require the CSP to delete the Data from the CSP's systems.

2. MARKET PROFILES[26]

AUSTRALIA

A. Who are the relevant Regulators?

- The Australian Prudential Regulatory Authority (www.apra.gov.au) ("**APRA**")
- The Australian Securities and Investments Commission (www.asic.gov.au) ("**ASIC**")
- The Office of the Australian Information Commissioner (www.oaic.gov.au) ("**OAIC**")

B. Introduction and Update

The Australian government remains optimistic about the role of cloud computing for the financial services sector. The Australian government is acting as a leader in its adoption with the Digital Transformation Agency (DTA) having released a new Secure Cloud Strategy on 1 February 2018.[27] This new strategy replaces the 2014 Australian Government Cloud Computing Policy and aims to increase the ease and rate of cloud adoption by government agencies. The DTA's review of the 2016 eCensus[28] also encourages the adoption of Cloud Services to boost cyber security in both the public and private sector.

Another recent development is the government announcement that Australians "should own their own data" and that the government would legislate a national *Consumer Data Right*.[29] This follows recommendations from the Productivity Commission's Data Availability and Use Inquiry released in May 2017.[30] The government expects that citizen data ownership will enable greater consumer choice and business transparency. However, there has been pushback from business groups claiming that such an initiative would incur significant costs for business as they would be required to store significant amounts of "consumer accessible" data. Should a citizen data ownership right become law in Australia, it's reasonable to expect that firms will be incentivised to adopt Cloud Services as they are required to store more consumer information. The further evolution of the government's position on open data may influence a regional approach to consumer data rights.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.** However, APRA's Information Paper on "Outsourcing Involving Shared Computing Services (Including Cloud)' outlines key principles to consider when availing of shared computing services.
3. Are there other regulations/guidelines that are relevant?	**Yes.** See next Section.
4. 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.

[26] 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 are not always the latest versions since they have not been updated periodically. Therefore, they should be used only for reference and should not be relied upon.
[27] https://www.dta.gov.au/news/new-strategy-for-cloud/
[28] http://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5/upload_pdf/Review%20of%20the%202016%20eCensus%20-%20final%20report.pdf
[29] https://ministers.pmc.gov.au/taylor/2017/australians-own-their-own-banking-energy-phone-and-internet-data
[30] https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf

5. 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.
6. Are there specific contractual requirements that must be adopted?	**Yes**. APRA requires that all outsourcing arrangements, including the outsourcing of information technology, must be evidenced by a written, legally binding agreement and must address at a minimum a number of issues set out in Clause 29 of the APRA Outsourcing Standard.
7. 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.

D. Relevant Regulations

Full Title and URL	Regulator, Abbreviated Title, and Citation/ Reference
APRA Prudential Standard Outsourcing	APRA: Outsourcing Standard, CPS 231
APRA Prudential Practice Guide: Outsourcing	APRA: Outsourcing Guide, PPG 231
APRA Prudential Practice Guide: Management of Security Risk in Information and Information Technology	APRA: Security Guide, CPG 234
APRA Prudential Standard CPS 232 Business Continuity Management	APRA: BCM Standard, CPS 232
Privacy Act 1988	OAIC: Privacy Act, No. 119, 1988
APRA Information Paper on Outsourcing Involving Shared Computing Services (Including Cloud)	APRA: Information Paper, 6 July 2015

E. Summary of the Key Requirements

Requirement and Summary	Citation
1. 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 Standard, Section 26
2. 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 23
3. 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 34
4. Confidentiality and security FSIs must ensure that CSPs implement an appropriate IT security risk management framework with the aim of maintaining confidentiality, integrity	APRA Security Guide Privacy Act, APP 11

Requirement and Summary	Citation
and availability, and adopt robust physical security controls 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.	
5. 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
6. 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 39
7. Data use CSPs must not use or disclose FSIs' Data for any purpose other than to provide the Cloud Services.	Privacy Act 1988, APP 6
8. Data segregation FSIs must put in place appropriate Data controls including Data segregation.	APRA Security Guide, Section 48
9. Subcontracting Cloud Contracts must include specific rules for, 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 standards 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 29 (n) APRA Outsourcing Standard, Section 29 (p), Section 34, Section 35
10. 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 29 (b) (k) APRA Security Guide, Section 55

HONG KONG

A. 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.ia.org.hk, 保險業監管局) ("**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**")

B. Introduction and Update

Hong Kong's financial services sector has benefited from technology-neutral outsourcing and TRM regulations, while recent regulatory developments have been supportive of the use of cloud and broader fintech development. The PCPD sought to help organisations (including FSIs) that outsource cloud understand their obligations in complying with privacy laws, through its July 2015 Cloud Computing Information Leaflet.[31]

More recently, the HKMA announced seven initiatives to support a "New Era of Smart Banking",[32] which bode well for cloud demand among Hong Kong FSIs. For example, one of the seven initiatives is a plan to upgrade the HKMA's Fintech Supervisory Sandbox (FSS). The FSS 2.0 will link the sandboxes of the HKMA, IA and Securities and Futures Commission (SFC) to simplify entry for cross-sector fintech pilots, while enabling tech companies to directly access the integrated sandbox, without having to first go through a partner bank. Another initiative that aims to encourage the adoption of innovative technology in the financial services sector is through the promotion of virtual banks, which entails a review process of the HKMA's 2000 Guide to Authorization of Virtual Banks,[33] with a revised guideline expected to be issued in May 2018.[34]

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.** However, the PCPD's Cloud Computing Information Leaflet provides specific guidance on complying with the PDPO's data protection principles when using Cloud Services.
3. Are there other regulations/guidelines that are relevant?	**Yes.** See next Section.
4. Is regulatory approval required?	**No.**
5. 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.
6. 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 HKMA Outsourcing and Technology Guidelines do contain guidelines on some contractual provisions that Banks may include in the 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

[31] https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf
[32] http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170929-3.shtml
[33] http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/guide-authorization/Chapter-9.pdf
[34] http://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180206-4.shtml

	list of matters that it says Insurers should "consider" when negotiating the contract.
7. Other information/ developments	In December 2014, the PCPD published a Guidance Note for cross-border data transfers. Although Section 33 of the PDPO, which prohibits the cross-border transfer of personal data unless one or more conditions are met, is not yet in force, this Guidance Note serves the purpose of helping data users prepare for the implementation of Section 33.

D. Relevant Regulations

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

E. Summary of the Key Requirements

Requirement and Summary	Citation
1. Due diligence Before selecting a CSP, Banks should perform appropriate due diligence, such as ensuring that the proposed outsourcing arrangement has been subject to a comprehensive risk assessment (in respect of operational, legal and reputation risks) and that all identified risks have been adequately addressed before launch. Before selecting a CSP, Insurers should perform due diligence on the CSP (including considering factors such as aggregate exposure to the CSP, possible conflict of interests, and price vis-à-vis the benefit gained in assessing and selecting a CSP). Before entering into a new outsourcing arrangement or renewing or varying an existing outsourcing arrangement, Insurers should conduct 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 ensure that all the risks identified have been addressed before launch.	HKMA Outsourcing Guidelines, Sections 2.2 and 2.3 IA Outsourcing Guidance, Sections 15 and 17
2. Review, monitoring and control Banks should have controls in place (e.g. comparisons with target service levels) to monitor the performance of CSPs on a continuous basis. Banks should 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 should 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 16
3. Audit Banks should 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 should not be impeded by the outsourcing. Insurers should consider allowing access by the auditors and actuaries of the Insurer and the IA to any books, records and information in its Cloud Contract.	HKMA Outsourcing Guidelines, Section 2.8 IA Outsourcing Guidance, Section 19
4. Confidentiality and security Banks should have controls in place to ensure that the requirements of Customer Data confidentiality are observed and proper safeguards are established to protect	HKMA Outsourcing Guidelines, Sections 2.5.1 and 2.5.2

Requirement and Summary	Citation
the integrity and confidentiality of Customer Data. Detailed guidelines must be followed as set out in the HKMA Technology Guidelines. Insurers should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements (e.g. PDPO) and common law customer confidentiality. Insurers should have controls in place to ensure requirements of Customer Data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of Customer Data.	IA Outsourcing Guidance, Sections 13 and 21 HKMA Technology Guidelines
5. Resilience and business continuity Banks should 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 should 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 should develop a contingency plan to ensure that its business would not be disrupted from undesired contingencies (e.g. systems failure) of the CSP.	HKMA Technology Guidelines, Section 7.1.1 HKMA Outsourcing Guidelines, Sections 2.7.1 and 2.7.2 IA Outsourcing Guidance, Section 26
6. Data location Outsourcing can be to a CSP in Hong Kong or overseas. Banks should give notice to customers of significant outsourcing initiatives, particularly where the outsourcing is to an overseas jurisdiction. Banks should 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 should understand the risks arising from overseas outsourcing, taking into account relevant aspects of an overseas jurisdiction (e.g. legal system, regulatory regime and the ability of the Insurers to monitor the Cloud Services and the CSP).	HKMA Outsourcing Guidelines, Section 2.5.3 and 2.9.1. IA Outsourcing Guidance, Section 28
7. Data use Data should 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
8. Data segregation Banks should 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
9. Subcontracting Banks should 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 should include in the Cloud Contract rules and restrictions on subcontracting and making the CSP liable for the capability of the subcontractor. The Insurer should 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
10. Termination In the event of a termination of the Cloud Contract, for whatever reason, FSIs should ensure that all Data is either retrieved from the CSP or destroyed.	HKMA Outsourcing Guidelines, Section 2.5.4 IA Outsourcing Guidance, Section 22

INDIA

A. Who are the relevant Regulators?

- The Reserve Bank of India (www.rbi.org.in) ("**RBI**") is the central bank and regulates FSIs. It lays down the legal framework for outsourcing of financial services, including the use of Cloud Services
- The Securities and Exchange Board of India (www.sebi.go.in) ("**SEBI**") regulates the securities market
- The Insurance Regulatory and Development Authority (https://www.irdai.gov.in) ("**IRDAI**") regulates the insurance and re-insurance industries
- The Ministry of Electronics and Information Technology (www.meity.gov.in) ("**MeitY**") is responsible for all policy matters related to information technology, electronics, and internet
- 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
- The Telecom Regulatory Authority of India (www.trai.gov.in) ("**TRAI**") regulates telecom services, with the aim to provide a fair and transparent policy environment which promotes a level playing field

B. Introduction and Update

The TRAI, on 2 February 2018, published its inputs on India's National Telecom Policy 2018 (NTP – 2018) including recommendations to incentivise the setting-up of International Data Centres (IDCs) and establishing India as a global hub for research and development, innovation and cloud computing.[35] The TRAI also released its Recommendations on Cloud Services in August 2017, in which it proposed a light touch regulatory approach in order to reduce the regulatory burden in adoption of cloud computing, and ensure that strict regulations do not stymie technological innovations in the cloud sector.[36] The TRAI acknowledged the need for a comprehensive legal framework for data protection when using Cloud Services to ensure the privacy of personal data. In this regard, the MeitY released a White Paper on a Data Protection Framework in India in November 2017, inviting public comments.[37] This data protection framework will play an important role in the adoption of cloud technologies in India. India is also witnessing cloud computing developments at the state level, with Maharashtra having released its Public Cloud Policy in January 2018, which mandates its government departments to shift their data storage onto cloud.[38]

This support for cloud is also evident in sector-specific guidance that directly applies to FSIs. In August 2017, the Institute for Development and Research in Banking Technology (IDRBT), an arm of the RBI, released its Cloud Adoption FAQs which list the benefits of the cloud and sets out to help FSIs on their journey to cloud adoption. Notably, the FAQs recognise that data security is not dependent on location, and that third-party audit reports can be relied on to authenticate a CSP's controls.

[35] As per the DoT's request, the TRAI held a consultation and invited comments on the NTP-2018 and subsequently published its inputs http://www.trai.gov.in/notifications/press-release/trai-releases-inputs-formulation-national-telecom-policy-2018
[36] http://trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf
[37] http://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited
[38] https://economictimes.indiatimes.com/tech/internet/maharashtra-becomes-the-first-state-to-unveil-public-cloud-policy/articleshow/62540943.cms

Furthermore, recent initiatives in India are indicative of the government's support in bringing about technological advancements in the financial services sector:

- The RBI set-up Reserve Bank Information Technology Pvt Ltd (ReBIT) to address the cyber security needs of the financial sector and aid research and technological innovation in the Indian banking industry.[39]
- Through fintech initiatives like Jan Dhan Yojana[40], Aadhaar[41], and the Unified Payments Interface (UPI)[42], the Government of India is working towards digitising payment systems and increasing financial inclusion.[43]
    - Jan Dhan Yojana, launched in August 2014, targets the under-banked and low-income groups, with effective use of technology.
    - Similarly, the Aadhaar biometric identification program aims to achieve social inclusion and efficient public and private service delivery.
    - The UPI platform, which was launched by the National Payments Corporation of India (NPCI) in August 2016, facilitates instant transfer of funds between bank accounts.
    - In December 2017, the NPCI established a framework for integrating non-bank mobile wallets with the UPI system.[44] This move, coupled with upcoming plans to also introduce a newer version of UPI (UPI 2.0) to allow users to pre-authorise transactions through digital signatures, aims to increase digital transaction volumes.

Given the current government's focus on building India's digital economy, an accelerated pace of the innovation in the financial services sector led by government initiatives can be expected going forward.

It is important to note, however, that data localisation demands, which have prevented cross-border transfers of public sector data since 2012,[45] are beginning to be applied to the private sector and the financial services sector is one of the first to be impacted. The RBI on 5 April 2018 issued a new requirement for all payment service operators to store their payments data within India by 5 October 2018. Paragraph 4 of the "Statement on Developmental and Regulatory Policies"[46] is aimed at giving the RBI unrestricted access to all payment data for supervisory and monitoring purposes in the context of ensuring the safety and security of payment systems. On 6 April 2018, the RBI followed up with a notification on "Storage of Payment System Data",[47] which explicitly states the requirement for RBI to be given access all forms of payment system data stored by service providers and other third-party vendors.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.** However, the IDRBT's "FAQs on Cloud Adoption for Indian Banks" can be used as a reference.
3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.

[39] https://www.rebit.org.in/
[40] https://pmjdy.gov.in
[41] https://uidai.gov.in
[42] https://www.npci.org.in/product-overview/upi-product-overview
[43] https://www.pwc.in/assets/pdfs/publications/2017/fintech-india-report-2017.pdf
[44] http://www.livemint.com/Industry/1Jm7bmdIAHqZhTxvZPkXQK/NPCI-working-on-integrating-nonbank-mobile-wallets-with-UPI.html
[45] http://www.dst.gov.in/sites/default/files/nsdi_gazette_0.pdf
[46] https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR264270719E5CB28249D7BCE07C5B3196C904.PDF
[47] https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

4. 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 D. **Notification.** Reporting is required for significant outsourcing arrangements and if data sharing is involved across geographic locations. See RBI Information Security Guidelines, p78.
5. 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 (although in some cases, notification is required – see above.) There is no form/questionnaire required to be completed. FSIs must exercise due diligence before entering into an outsourcing arrangement and comply with the requirements outlined in Section D.
6. Are there specific contractual requirements that must be adopted?	**Yes.** The outsourcing contract must have specific clauses relating to confidentiality, auditing, monitoring, termination, performance standards, dispute resolution, subcontracting and customer rights etc. See next Section for specific examples.
7. Other information/ developments	In 2013, the Government of India launched a cloud computing initiative called "GI Cloud" (coined "Meghraj") to formulate and implement a Cloud Policy and increase the use of Cloud in government. MeitY has set-up a working group to examine a number of regulatory and operational aspects of cloud computing such as jurisdiction, cross-border data flow, data security, and data location. MeitY also maintains a list of empanelled CSPs, to be part of the GI Cloud Services Directory. Further to the GI Cloud initiative, TRAI published its Recommendations on Cloud Services in 2017, which proposes a light touch regulatory framework to regulate Cloud Services in India. This approach aims to protect the interests of the users of Cloud Services and to also ensure that technological and business advancements in the cloud sector are not thwarted by strict regulations. Once approved by DoT, the recommendations outlined below are likely to be implemented: i. TRAI recommends that DoT prescribe a framework to register CSPs whereby CSPs operating in India would collaborate to form an "industry body for Cloud Services in India". There will be no restrictions on the number of such industry bodies. ii. DoT may issue directions to such industry bodies, and may also withdraw or cancel the registration of an industry body if instances of breach and non-compliance occur. iii. This industry-led body for Cloud Services will prescribe a code of conduct (CoC) of their functioning with certain provisions including the adoption of a constitution, creation of working groups, putting in place a dispute resolution framework, formulating a model Service Level Agreement (SLA), among others (Detailed provisions in Section 3.10). iv. All CSPs above a threshold value who have been notified by the government from time to time in the previous financial year have to become a member of one of the registered industry bodies for Cloud Services and accept the prescribed CoC. The threshold may be based on either volume of business, revenue, number of customers, etc. or a combination of all these. v. An oversight body, Cloud Service Advisory Group (CSAG), will be created to periodically review the progress of Cloud services and suggest any government actions that are required to be taken. This Advisory Group may consist of Representatives of state IT departments, Small and Medium Enterprises associations, Consumer advocacy groups, Industry experts, and Representatives of Law Enforcement agencies.

D. Relevant Regulations

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
Cyber Security Framework in Banks	RBI: Cyber Security Framework, RBI/2015-16/418 DBS.CO/CSITE/BC.11/ 33.01.001/2015-16
Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks	RBI: Outsourcing Guidelines, RBI/2006/167 DBOD.NO.BP. 40/ 21.04.158/ 2006-07
Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds	RBI: Information Security Guidelines, RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11
The Information Technology (Amendment) Act, 2008	IT Amendment Act, 5th February, 2009/Magha 16, 1930 (Saka)
Information Technology Act, 2000	IT Act, 9th June, 2000/Jyaistha 19, 1922 (Saka)
Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011	MeitY: Privacy Rules, GSR 313(E), dt 11-4-2011
Information Technology (Intermediaries Guidelines) Rules, 2011	MeitY: Intermediary Guidelines, GSR 314(E), dt. 11-4-2011
Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks	RBI: Credit Cards Circular, RBI/2014-15/58 DBOD.No.FSD.BC.02/ 24.01.009/2014-15
Credit Information Companies (Regulation) Act, 2005 and Credit Information Companies Rules, 2006	Credit Information Companies Act and Rules, G.S.R.754 (E). dt. 14-12-2006
Revised Terms and Conditions - Other Service Provider (OSP) Category	DoT: SP Terms, No.18- 2/2008-CS-I dt. 5-08-2008
SEBI Master Circular for Depositories	SEBI: Master Circular, SEBI/HO/MRD/DP/CIR/P/2016/134, December 15, 2016
IDBRT FAQs on Cloud Adoption for Indian Banks	Cloud Adoption FAQs, August 2017

E. Summary of the key requirements

Requirements and Summary	Citation
1. 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 services and 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. It is a requirement to inform the Indian Computer Emergency Response team in the case of any cyber security incidents and appoint a Grievance Officer to address complaints from users. The Intermediary Guidelines also state that an FSI	Outsourcing Guidelines, Paragraphs 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

Requirements and Summary	Citation
must not knowingly deploy, install or modify the technical configuration of any computer resource to change the course of its operations.	
2. 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, Paragraphs 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, Paragraphs 8 and 15
3. 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 (by internal or external auditors) 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 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.	Outsourcing Guidelines, Paragraphs 2, 4.4, 5.5.1 and 5.9 of the Annexure Information Security Guidelines, Chapter 4 and Chapter 5
4. Confidentiality and security Banks should put in place a comprehensive Board approved cyber security policy, and implement appropriate measures to protect customer information, irrespective of whether the data is stored/in transit within the Bank or with third party vendors such as CSPs. As per the IT Act, any "body corporate", including CSPs, which processes sensitive personal information is required to ensure that adequate data protection mechanisms are in place. If any negligence in this regard occurs, the body corporate will be liable to pay damages to the affected person. 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;	Cyber Security Framework, Paragraph 10 IT Amendment Act, Section 43A Privacy Rules, Rule 4 and Rule 8 Outsourcing Guidelines, Paragraphs 4.1, 5.5.1 and 5.6 of the Annexure Information Security Guidelines, Chapter 2 and Chapter 4 Intermediary Guidelines, Rule 4

Requirements and Summary	Citation
• 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.	Credit Information Companies Act, Chapter VI and Credit Information Rules, Chapter III, IV, V and VI Credit Cards Circular, Paragraphs 6.1, 6.2 and 15
5. 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, Paragraphs 5.8 and 5.6.3 of the Annexure Information Security Guidelines, Chapter 4 and Chapter 7 SEBI Master Circular, Section 4.19
6. 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 are 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. SEBI also requires that disaster recovery sites should be located in a different seismic zone from the primary data centre.	Privacy Rules, Rule 3 and Rule 7 Outsourcing Guidelines, Paragraph 7.4 of the Annexure Information Security Guidelines, Chapter 4 SEBI Master Circular, Section 4.19.iii
7. 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. CSPs will be held liable for disclosure of any information in breach of a lawful contract. While providing services under the terms of a legal contract, any person who secures access to personal information about another person, with the intent to cause harm, and without the consent of the person concerned, shall be punished with imprisonment for a term up to three years, or with a fine up to five lakh rupees, or with both.	Privacy Rules, Rule 5 and Rule 6 Outsourcing Guidelines, Paragraph 5.5, of the Annexure IT Amendment Act, Section 72A
8. 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
9. 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

Requirements and Summary	Citation
	Information Security Guidelines, Chapter 4
10. 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

Case Study:

India's YES BANK

YES BANK is a private bank with 1,000 branches in over 670 locations and more than 20,000 employees in India. YES BANK's continuous innovation and investment in technology platforms has enabled it to sustain its competitive advantage, helping it become one of the fastest growing banks in India.

YES BANK was keen on deploying a communication platform that, unlike typical business applications, had a familiar chat-like interface similar to the social and messaging tools that have become an integral part of people's daily lives. This led to the adoption of Microsoft's mobile and communications app Kaizala, which is powered by Microsoft Azure. The cloud-based app allowed the bank to develop multiple enterprise-to-employee, business-to-business and business-to-consumer uses, including:

- Public groups for dissemination of information to customers
- Digitalisation of most frequently used service requests/complaints for customers
- Private groups based on the organisational hierarchy for knowledge and information dissemination
- Daily sales report with capabilities such as auto roll-up for a real-time view of progress
- Unit visit reports with capabilities to document discussion pointers, attach documents, geo-tag locations, ensuring all information is captured digitally
- Digitising forms like Point of Sale (POS) enablement for Current Account customers

Enhancing sales team productivity

Kaizala's capabilities, which include the ability to create natural work groups and hierarchies, manage group members, and upload information that is appropriate to the relevant audience, provided the Human Capital Management (HCM) unit of YES BANK with a platform for effective organisational communication.

This allowed YES BANK to quickly create user groups based on existing hierarchies that reflected the organisational structure of its real-world sales team. The communications app's flexible survey and poll features then doubled up as smart data collection forms. The typical sales cycle that involved manual work of gathering information and updating the system with it previously took about a day and a half. Deploying to a cloud computing platform allowed for real-time data collection and access to information, which enabled YES BANK to realise up to two to three times in productivity gains.

Enabling a self-service channel to increase customer satisfaction

By connecting its network of customers and partners, YES BANK has simplified and streamlined the process of coordinating POS functions between the bank, merchants and POS vendors. Retail customers will soon be able to request services such as cheque book ordering and duplicate bank statements via the chat app through an API-based integration of Kaizala with YES BANK's Customer Relationship Management (CRM) system. YES BANK also has plans to use the app as a platform for merchant partners to raise incident or service requests, which the bank can then quickly respond to.

Source: Thanks to Microsoft for providing this case study. For more information, visit https://customers.microsoft.com/en-ca/story/yes-bank-kaizala-power-bi-en

INDONESIA

A. Who are the relevant Regulators?

- Bank of Indonesia (www.bi.go.id, Bank Sentral Republik Indonesia) ("**BI**")
- The Financial Services Authority of Indonesia (www.ojk.go.id, Otoritas Jasa Keuangan) ("**OJK**")
- Ministry of Communication and Information Technology (www.kominfo.go.id, Kementerian Komunikasi dan Informatika Republik Indonesia) ("**Kominfo**")

B. Introduction and Update

Indonesia has neither a formal cloud first policy, nor a coordinated initiative for the adoption of cloud within the public sector. Whilst there is no government moratorium against the adoption of cloud in the public sector, the Indonesia Broadband Plan 2014-19[48] called for a shift to government-wide data centres based nationally. This is illustrative of the Indonesian government's approach to cloud computing; it is acceptable so long as the data centre is based in Indonesia, and auditable by the relevant regulators.

Indonesian regulation since 2013 has seen the OJK take on the authority over bank supervision and regulation from the BI. Old BI regulations were superseded by a newer OJK regulation in December 2016. New regulation POJK38/2016 states that commercial banks and commercial Shariah banks must report and obtain consent from OJK for any outsourcing arrangements. Furthermore, these banks cannot store any personal or transaction data offshore, and must submit a statement letter to the OJK, permitting the regulator to audit their CSP at any time. POJK38/2016 also requires FSIs to keep data centre and disaster recovery facilities onshore. Similar regulatory provisions have been made for insurance companies under Regulation POJK69/2016. Rural and rural Syariah banks have also been targeted under POJK75/2016, which states that data centres need to be located within Indonesia, and in a location with a different risk profile to that of the disaster recovery centre.

2017 saw the establishment of the National Payment Gateway (NPG) in Indonesia. This prescribes that all data generated by e-payments must be processed through any one of four NPG "switching agency" companies that have been selected by the government. Furthermore, all payment card companies will need to route all domestic transactions through the NPG as of June 2018. Furthermore, BI Circular No. 17/52/DKSP requires all magnetic stripe-based debit transactions to be processed and stored domestically. Debit transactions are to be processed domestically by 1 January 2022.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.**
3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.
4. Is regulatory approval required?	**Yes.**
5. Is there a process to follow? If so what is the process and is	**Yes for commercial banks, otherwise no.** Commercial banks[49] must report on any intended outsourcing arrangements to the OJK and

[48] https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/Sep-WABA/Presentations/Indonesia%20Broadband%20Plan%20(ITU%20Jakarta,%20090915).pdf

there a specific form/ questionnaire to be completed?	obtain approval. Cloud Services would be considered outsourcing arrangements subject to this approval requirement. Commercial banks must complete and submit an application to OJK as part of the approval process which includes summaries of reports, various letters and plans.
6. 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 Article 20 of POJK38/2016 and Section 9.2.2(c) of 21/SEOJK.03 / 2017. See next Section for some examples.
7. Other information/ developments	There is no official Data Protection Act. However, a draft Bill on the Protection of Personal Data is currently under debate and may soon be passed. A 2016 amendment has been made to the 2008 ITE Law; introducing the "right to be forgotten" for individuals. Further and more specific protections of personal data have been put in place by Kominfo's Regulation No.20 of 2016. Breach of such regulations can result in administrative sanctions from warnings to temporary suspension of business. The OJK and the BI have developed distinct roles since the 2015 report. BI is now in charge of e-money, e-payments, and the NPG. OJK remains in charge of all other affairs including outsourcing arrangements and e-banking. Both OJK and BI retain the authority to issue their own regulations. BI released regulation 19/12/PBI/2017 in November 2017, which aims to encourage innovation in the fintech industry while limiting the risks to the stability of the monetary system. OJK had planned to follow suit with a new fintech regulation by March 2018. The NPG requires all e-transaction data to be processed locally through "switching agencies" selected by the Indonesian government as of June 2018.

D. Relevant Regulations

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
Indonesian Banking Law	OJK Law No. 10 of 1998, Law No. 10 of 1998
Law No. 11 of 2008 on Electronic Transaction and Information	Kominfo ITE Law, Law No. 11 of 2008
Government Regulation No. 82 of 2012 on Electronic System and Transaction	Kominfo GR 82, GR No. 82/2012
Regulation of OJK No. 38/POJK.03/2016 on Risk Management on Information Technology Use by Commercial Banks	OJK POJK38/2016, 38/POJK.03/2016
OJK Circular Letter 21 / SEOJK.03 / 2017 of 6 June 2017 on Risk Management in Use of Information Technology by Commercial Banks	OJK 21/SEOJK.03/ 2017, 21/SEOJK.03/ 2017
Regulation of OJK No. 69/POJK.05/2016 on Business Operation of Insurance, Sharia Insurance, Reinsurance and Sharia Reinsurance Companies	OJK POJK69/2016, 69/POJK.05/2016
Regulation of OJK No. 77/POJK.01/2016 regarding Technology-Based Fund-Lending Services	OJK POJK77/2016, 77/POKK.01/2016
Regulation of OJK No. 75 /POJK.03/2016 about Standard of Information Technology Information For Rural and Sharia Funding Bank	OJK POJK75/2016, 75/POJK.03/2016
BI Circular No.17/52/DKSP	BI Circular No.17/52/DKSP

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
BI Regulation No.19/12/PBI/2017 on the Implementation of Financial Technology[50]	BI 19/12/PBI/2017, 19/12/PBI/2017
Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems	Kominfo No.20 of 2016, No. 20/2016
National Payment Gateway	Kominfo GPN, No. 19/49/DKom

E. Summary of the Key Requirements

Requirements and Summary	Citation
1. Due diligence Commercial Banks are responsible for implementing risk management measures for their use of IT service providers. Commercial banks are required to conduct a thorough due diligence process when choosing between CSPs. The scope of the due diligence should cover relevant issues, including the CSP's reputation, technical capability, operational capability and financial condition, innovativeness, necessary for the commercial bank to assess whether the CSP can meet its requirements.	POJK38/2016, Article 20(3), 21/SEOJK.03/ 2017, Section 9.2.3(c)
2. Review, monitoring and control Commercial banks are required to monitor and evaluate the reliability of their CSP periodically in respect of their performance, reputation and continuity of service provision. The commercial bank should have a monitoring program to ensure that the CSP has performed the work or provided its services in accordance with the terms of the Cloud Contract. The resources to support this program may vary depending on the criticality and complexity of systems, processes and services of the CSP. The due diligence performed by the commercial bank on the CSP during the selection process must be regularly re-performed as part of the bank's monitoring process.	POJK38/2016, Article 20(3) 21/SEOJK.03/ 2017, Section 9.2.3 and 9.4.1
3. Audit As part of their broader risk management and internal IT audit requirements, commercial banks are required to perform audit functions on the CSP periodically. These audits can be performed by either the commercial bank's internal auditors or external auditors. The areas to be audited include the IT system, data security, internal control framework, and disaster recovery plan. The commercial bank must ensure that OJK is provided with the results of the bank's review and findings on the CSP that are related to the IT services. The Cloud Contract should include terms allowing for either internal commercial bank's auditors, OJK or an external auditor appointed by the bank or OJK to have access to information of the commercial bank for inspection purposes, including access rights, logically and physically, to the data of the commercial bank.	POJK38/2016, Article 18 POJK3/2016, Article 19 (2-4) 21/SEOJK.03/ 2017, Section 9.4.2 21/SEOJK.03/ 2017, Section 9.2.2(c)(13)
4. Confidentiality and security Data, particularly data relating to the commercial bank's customers, must only be accessible by the commercial bank. The Cloud Contract should set out security standards that will be complied with by the CSP. The bank should ensure that the CSP has security controls in place for mitigating risks including background checks on its staff, security of IT facilities and ability to facilitate the level of data security required by the bank.	21/SEOJK.03/ 2017, Section 9.2.2(c)(4) and 9.2.2(c)(24) and 9.3.4
5. Resilience and business continuity The commercial bank should ensure that it has a disaster recovery plan and periodically test this plan. As a matter of risk mitigation, the commercial bank	21/SEOJK.03/ 2017, Section 9.2.2(c)(16), Section 9.2.3(d)(4),

[50] Together with No.19/12/PBI/2017, BI also released regulations No.19/14/PADG/2017 (http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/PADG_191417.aspx) and No.19/15/PADG/2017 (http://www.bi.go.id/id/peraturan/sistem-pembayaran/Pages/PADG_191517.aspx) that explain the implementation of a regulatory sandbox and registration for fintech companies in detail.

Requirements and Summary	Citation
should ensure that the CSP has a disaster recovery plan commensurate with the type, scope and complexity of the activities or services provided. The commercial bank must ensure that the CSP can provide independently audited results on the data center and/or disaster recovery centre. CSPs should test their own IT systems and facilities and the results of their tests should be used by the commercial bank to update its own disaster recovery plan.	Section 9.3.3 (c) and (d) POJK38/2016, Article 20 (3)(i)
6. Data location Commercial banks should place their data centre and disaster recovery centre in Indonesia unless OJK approves otherwise. IT-based lenders (e.g. peer to peer lenders) are required to use a data centre and disaster recovery centre in Indonesia. Insurance companies are required to place certain categories of data in a data centre and disaster recovery centre in Indonesia for the purposes of law enforcement and state sovereignty. These categories are data and information relating to the personal data of policyholders, premium payment transactions or claims, administrative data and the administration of the insurance company. Offshoring personal data requires coordination with Kominfo.	POJK38/2016, 21 POJK77/2016, Article 25 POJK69/2016, Article 49 and 50 No. 20 of 2016
7. Data use Commercial banks are required to ensure that their Cloud Contracts include commitments on data confidentiality.	21/SEOJK.03/ 2017 Section 9.2.2(c)(4) POJK38/2016, Article 20 (3)(i)
8. Data segregation There are no specific requirements.	N/A
9. Subcontracting CSPs may subcontract part of their services only with a written agreement of the commercial bank.	POJL38/2016 Article 20 (3)(i) 21/SEOJK.03/ 2017, Section 9.2.2(c)(9)
10. Termination Commercial banks must have the ability to terminate their Cloud Contract early. The OJK must also be able to instruct the commercial bank to terminate the Cloud Contract prior to the expiration of its term.	21/SEOJK.03/ 2017, Section 9.2.2(c)(21)

Case Study:

Indonesia's Bank Central Asia

Bank Central Asia (BCA) is a private bank headquartered in Jakarta which offers business transactions, credit loans, and financial solutions. Its service delivery infrastructure includes 1,213 branches, 17,207 ATMs, more than 400,000 electronic data capture (EDC) machines, and 24-hour Internet and mobile banking.

BCA was looking to accelerate its service innovation and increase its operational agility and responsiveness, while protecting sensitive client and financial data and maintaining a high level of availability. This led it to adopt Cisco's software-defined networking (SDN) solution to increase software flexibility and performance scalability.

Addressing the challenge of accelerating banking innovation

To reduce manual tasks and accelerate innovation, BCA adopted Cisco Application Centric Infrastructure (Cisco ACI) in December 2015. The SDN solution allowed it to implement policy-based automation and centralised management to its banking network and 50 core applications.

This enabled BCA's entire network environment to be managed from a single console, speeding up infrastructure deployments and allowing BCA to better adapt to changing business, customer and application development needs. For example, BCA used to spend several days manually adjusting servers, switches and VLANs to prepare for long public holidays, when the closure of branch locations would result in additional and short-term 10-20% increase in Internet and mobile banking demand. Moving to cloud computing infrastructure thus allowed BCA to make adjustments in minutes without needing any physical changes to the infrastructure.

BCA Task	Before	After
Server connectivity	Configuration on each switch or router	Configuration through centralised console
Virtual Machine (VM) connectivity	5 manual processes	3 manual processes
New VM server for existing application	10 to 20 minutes	10 seconds
Endpoint physical port tracing	5 to 10 minutes	30 seconds
Capacity measuring	10 to 30 minutes	20 seconds
Network configuration	Manual	XML/ JSON scripting through PAI

Improving security and troubleshooting

The implementation of Cisco ACI improved infrastructure visibility by bringing down technological and procedural walls that previously separated operations, server and application teams, while strengthening BCA's overall security posture. Connections cannot be established without explicit, policy-based instruction, providing granular segmentation and control that can be extended across multiple environments, and improving BCA's ability to protect and manage its foundational technologies and data resources.

By enabling BCA's IT operations team to see where all of the bank's physical and virtual components are located, the team can also quickly identify and address problems from their root cause by tracing application and data flows from back-end systems to customer-facing channels. This reduced the time taken to troubleshoot tasks from 10 minutes or more to just seconds.

Such efficiency gains also spawned a cultural shift within the bank's IT organisation by freeing up time previously spent fulfilling requests from the server and application teams and instead allowing resources to be directed towards exploring new products and features.

Source: Thanks to Cisco for providing this case study. For more information, visit https:// cisco.com/c/en/us/about/case-studies-customer-success-stories/bank-central-asia.html

MALAYSIA

A. Who are the relevant Regulators?

- Bank Negara Malaysia (www.bnm.gov.my) ("**BNM**")
- Personal Data Protection Commission (www.pdp.gov.my) ("**PDPC**")

B. Introduction and Update

Malaysia's private sector has been receptive to cloud adoption, and the government's announcement on 19 October 2017 to introduce a Cloud First Strategy is telling of an increasingly pro-cloud stance from the public sector.[51] While no further details have been disclosed, this decision to apply a government-wide Cloud First approach has sent a strong signal of federal support for cloud.

Efforts to improve technological adoption in the financial services sector have also been undertaken by the BNM; for example, the Financial Technology Regulatory Sandbox Framework,[52] released in October 2016, aims to provide a conducive regulatory environment for fintech companies. It moots a possible review of regulatory requirements that may be inhibiting innovation. The Financial Technology Enabler Group (FTEG), a group within BNM, was also set up in March 2017 to oversee technological innovation in FSIs, and is exploring the possibility of enabling the use of cloud for secure data storage for fintech companies.[53]

However, there are upcoming regulations that could potentially negate much of Malaysia's efforts to promote the use of innovative technologies in FSIs, including cloud. For example, BNM's new overarching Outsourcing Draft primarily seeks to implement higher standards of governance and more stringent outsourcing risk management measures among regulated entities. At the same time, it also imposes some restrictive requirements including the need for FSIs to seek prior regulatory approval on all outsourcing arrangements, data localisation, and for CSPs to award FSIs rights to conduct audits on their data centre facilities (see next Section for more detail). These new requirements are neither conducive for FSIs' cloud adoption nor the operating environment of their CSP partners, and may undermine other efforts to promote the use of Cloud Services in Malaysia's financial services sector.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.**
3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.
4. 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 outsourcing must be notified to BNM.
5. 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.

[51] https://www.pmo.gov.my/home.php?menu=newslist&news_id=19721&news_cat=13&cl=1&page=1731&sort_year=&sort_month
[52] http://www.bnm.gov.my/index.php?ch=57&pg=137&ac=533&bb=file
[53] http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=721

6. 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 C.
7. Other information/ developments	On 7 December 2017, BNM released its Interoperable Credit Transfer Framework (ICTF) Exposure Draft, which had the aim of facilitating collaborative competition between banks and non-bank e-money issuers. However, the draft imposes a localisation requirement on customer data, potentially restricting cloud adoption among payment infrastructure providers. On 27 September 2017, BNM published its Exposure Draft on Outsourcing for public comment. The Outsourcing Draft seeks to streamline the current fragmented outsourcing regulatory approach and implement more stringent controls on outsourcing arrangements. The new overarching Outsourcing guideline will replace all other Outsourcing guidelines in Section C. If implemented in its existing state, the Outsourcing Draft could unintentionally erect barriers to FSI cloud adoption. For example, the Outsourcing Draft subjects all outsourcing arrangements and sub-contracting arrangements to regulatory approval, imposes a maximum period of three years on Cloud Contracts, and requires CSPs to allow an FSI and its external auditor the rights to conduct physical audits on the CSP's premises and systems.

D. Relevant Regulations

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

Note: BNM's Outsourcing Exposure Draft regulation, released on 27 Sep 2017, supercedes a number of policy documents listed above if implemented.

E. Summary of the key requirements

Requirements and Summary	Citation
1. 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.	BNM Outsourcing Guidelines (Banking), Paragraph 4.1(i) BNM IT Management Guidelines, Paragraph 15(a), Part II BNM Outsourcing Guidelines (Insurers), Paragraph 10.4

Requirements and Summary	Citation
	BNM E-Banking Guidelines, Paragraph 13.3(b)
2. 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 proper reporting and monitoring procedures over the integrity and quality of work conducted by a CSP. 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. 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.	BNM E-Banking Guidelines, Paragraph 13 BNM Outsourcing Guidelines, Paragraph 47.1(vi) BNM Data Management Guidelines, Paragraph 4.12 Internet Insurance Guidelines, Paragraphs 26.1(c) and(d) BNM Outsourcing Guidelines (Insurers), Paragraph 10.14
3. Audit CSPs must provide insurers and BNM with a right of audit. CSPs must provide audit and inspection rights to the insurer to evaluate the services provided, or alternatively, have an independent auditor evaluate them on its behalf. The FSI's internal auditor or other independent party appointed must be able to review the business continuity program and disaster recovery program of the CSP.	BNM BCM Guidelines, Paragraph 112 BNM E-Banking Guidelines, Paragraph 13.3(f) BNM IT Management Guidelines, Paragraph 15(c), Part II and Paragraph 1(c), Part V BNM Internet Insurance Guidelines, Paragraph 26.1(e) BNM Outsourcing Guidelines (Insurers), Paragraph 10.10(i)
4. Confidentiality and security Banks must obtain from the CSP a written undertaking to comply with the secrecy provision pursuant to Section 97 of the Banking and Financial Institutions Act. 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 CSP 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.	BNM Outsourcing Guidelines (Banking), Paragraph 7.1(iii) PDPA, Section 9 BNM E-Banking Guidelines, Paragraphs 13.3(d) and (e) BNM IT Management Guidelines, Paragraph 15(b), Part II BNM Internet Insurance Guidelines, Paragraph 26.1(f) and (g) BNM Outsourcing Guidelines (Insurers), Paragraph 10.10(e)

Requirements and Summary	Citation
Insurers must ensure that the service agreements with the CSPs shall contain obligations of the CSPs to protect confidential information, including provisions prohibiting the CSP 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. The agreement should include a provision requiring the insurer to be notified of any breach of confidentiality and address liability for losses that might result.	
5. 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' operations. 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 FSI or insurer should be notified in the event that the CSP makes significant changes to its contingency plans. FSIs must also have a contingency plan in the event that the arrangement with the CSP is suddenly terminated.	BNM BCM Guidelines, Paragraphs 111, 113 and 114 BNM E-Banking Guidelines, Paragraph 13.3(g) BNM Outsourcing Guidelines (Insurers), Paragraph 10.10(g) BNM Outsourcing Guidelines (Banking), Paragraph 4(ix)
6. 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 be processed in any different a manner than it would if it were processed in Malaysia so as not to contravene the PDPA.	PDPA, Section 129
7. 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
8. Data segregation The CSP must be able to isolate and clearly identify the FSI's Data, documents, records and assets to protect their confidentiality.	BNM E-Banking Guidelines, Paragraphs 20.2 and 20.3 BNM IT Management Guidelines, Paragraph 15(b), Part II BNM Outsourcing Guidelines (Insurers), Paragraphs 10.10(c) and (e)
9. 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.	BNM Outsourcing Guidelines (Insurers), Paragraph 10.10(k)

Requirements and Summary	Citation
10. 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.	BNM Outsourcing Guidelines (Banking), Paragraph 4(v) BNM Outsourcing Guidelines (Insurers), Paragraphs 10.6 and 10.10(i)

NEW ZEALAND

A. 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)

B. Introduction and Update

New Zealand has adopted a consistently positive approach to cloud computing in the financial services sector. The government maintains a Cloud First policy, through which it seeks to be open to the benefit from emergent technologies and act as a leader in cloud adoption.[54] Changes to cloud-relevant regulation affecting FSIs have been limited since 2015. Whilst New Zealand's RBNZ Outsourcing Policy and Privacy Act have since been updated or amended, the changes have not significantly impacted FSIs' ability to adopt cloud. The September 2017 amendment of the RBNZ Outsourcing Policy strengthened contractual provisions for outsourcing arrangements, instituted a formal definition of outsourcing, as well as a formal engagement process with the RBNZ on new proposed outsourcing arrangements. While the RBNZ maintains a white list of pre-approved functions and services that are excluded from the formal engagement process,[55] this stands to limit the adoption of cloud and other innovative technologies which are not included in the list.

However, it is worth noting that a significant amendment to the Privacy Act and mandatory data breach reporting law may be implemented in the near future. Recommendations from Privacy Commissioner John Edwards' 2017 paper on the proposed amendments to the Privacy Act,[56] if followed by the government, will give individuals ownership over their personal data; presumably in a similar manner as the movement in Australia. The proposed amendments will also ensure that firms minimise risk to individuals by "de-identifying" data that they wish to present to the public. Both recommended measures have potential to raise compliance costs for FSIs and may drive FSIs to adopt Cloud Services to cope with new obligations to retain more consumer data.

Also of importance is the government's recommendation for the adoption of mandatory data breach reporting laws, which may increase costs for CSPs. Currently, organisations are encouraged, but not obliged, to report data breaches.[57] However, changes were flagged as government acknowledged recommendations for such laws in the 2011 Law Commission's privacy law review.[58] Consequently, it is likely that New Zealand will adopt some mandatory reporting laws, given both global and regional trends: the European General Data Protection Regulation (GDPR), and Australia's recent implementation of mandatory data breach reporting laws have created a strong precedent for New Zealand to follow.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.**
3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.

[54] https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/why-agencies-must-use-cloud-services/
[55] https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Policy-development/Banks/Outsourcing-policy-for-registered-banks/Completed/2017%2009%2019%20-%20White%20list%20for%20the%20purposes%20of%20BS11.pdf?la=en
[56] https://www.dlapiper.com/en/newzealand/insights/publications/2017/03/proposed-amendments-nz-privacy-law/
[57] https://www.privacy.org.nz/further-resources/knowledge-base/view/331?t=35448_46106
[58] https://privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform/new-zealand-law-commission-privacy-review/

4. Is regulatory approval required?	**No.** The RBNZ does not require approval before FSIs in New Zealand outsource certain IT functionality to a CSP.
5. 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.
6. 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.
7. 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.

D. Relevant Regulations

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
RBNZ Outsourcing Policy September 2017 Revision	RBNZ: Outsourcing Policy, BS 11
Privacy Act 1993	PC: Privacy Act, 1993 No. 28

E. Summary of the key requirements

Requirements and Summary	Citation
1. 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: B1
2. 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 out by a person other than the FSI. This has to be sufficient to achieve the FSI's core functions under normal business conditions and in the event of stress or failure of the FSI or of a CSP to the FSI.	RBNZ Outsourcing Policy, Sections: B2,B3,B4,B5
3. Audit The RBNZ suggests, but does not require, that the audit and monitoring process of the CSP is included in the Cloud Contract. However, the RBNZ does not prescribe any audit process or audit rights.	RNBZ Outsourcing Policy Section: B4
4. Confidentiality and security FSIs must ensure Personal Data is protected, by security safeguards as it is reasonable to take in the given circumstances, against: loss; access, use, modification, or disclosure, except with the authority of the agency that holds the information; and other misuse.	Privacy Act, Principle 5
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 the risk that might interrupt the operation and management of the FSI for a material length of time. Banks must establish separation plans, to come into effect in the event of a disaster. Furthermore, the level of service a bank must provide in the occasion of a separation should be specified.	RBNZ Outsourcing Policy Section: B2,B5
6. 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

Requirements and Summary	Citation
7. 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
8. Data segregation There are no specific requirements.	N/A
9. Subcontracting There are no specific requirements.	N/A
10. Termination There are no specific requirements.	N/A

PHILIPPINES

A. Who are the relevant Regulators?

- Bangko Sentral ng Pilipinas (www.bsp.gov.ph) ("**BSP**") is the central bank of the Philippines
- The Department of Information and Communications Technology (www.dict.gov.ph) ("**DICT**") promotes national ICT development agenda, and is also responsible for cybersecurity and cybercrime

B. Introduction and Update

The Philippines government has indicated its strong support for the use of cloud by the release of its Cloud First Policy in January 2017. This DICT circular on "Prescribing the Philippine Government's Cloud First Policy" instructs all government agencies to consider cloud computing as the preferred ICT deployment strategy[59] so as to tap the benefits of the cloud including reduced IT management costs and increased service delivery efficiency.

Similarly, the case for technological adoption to drive efficiency is also apparent in the Philippines' financial services sector. One example is the BSP's Philippine Electronic Fund Transfer (EFT) System and Operations Network (PESONet), which was launched on 8 November 2017.[60] With the goal of moving from a "cash-heavy" to a "cash-light" economy, PESONet, which is the first automated clearing house (ACH) under the National Retail Payment System (NRPS), aims to facilitate seamless electronic payments among accounts in BSP-supervised financial institution (BSFIs). With only 63.8% of cities/municipalities in the Philippines having a banking presence as per BSP's report on "Financial Inclusion Initiatives 2016", there is scope for similar fintech efforts to increase financial inclusion and bring more people into the digital economy.[61]

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.** However, as per BSP's outsourcing guidelines, Banks are prohibited from outsourcing inherent banking functions such as granting of loans, position-taking and market risk-taking activities, managing of risk exposures, and strategic decision-making.
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.** However, the DICT issued a circular in 2017 to prescribe the Philippine government's Cloud First Policy directing all government agencies to adopt cloud computing as the preferred ICT deployment strategy.
3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.
4. Is regulatory approval required?	**Yes.** BSP is aware of the general trend of FSIs wishing to use Cloud Services. As a general guideline, 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. But, this does not apply to all FSIs. Banks may outsource activities without BSP approval as long as they have a CAMELS (Capital, Asset, Management, Earnings, Liquidity and Sensitivity to market risk) composite rating of at least 3 and Management rating of not lower than 3. Banks that do not meet these criteria are required to take prior approval from BSP, which will make a decision based on the bank's ability to manage risks associated with outsourcing.

[59] http://www.dict.gov.ph/wp-content/uploads/2017/02/Signed_DICT-Circular_2017-002_CloudComp_2017Feb07.pdf
[60] http://www.bsp.gov.ph/publications/media.asp?id=4529
[61] http://www.bsp.gov.ph/downloads/Publications/2016/microfinance_2016.pdf

5. 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.
6. 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.
7. Other information/ developments	BSP plans to issue enhanced IT risk management guidelines for all its supervised banks and financial institutions. The BSP governor, Nestor Espenilla Jr., has indicated that the new circular will present a more holistic information security management framework, covering cyber security, encryption standards, and cloud computing. At time of printing, the proposed reforms were under legal review after having been presented to major stakeholders, after which they will next be submitted to the Monetary Board for approval. No specific date for the official release has been set.

D. Relevant Regulations

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
Enhanced Guidelines on Information Security Management	BSP: Information Security Guidelines, Circular No. 982, Series of 2017
Amendments to the Guidelines on Outsourcing	BSP: Outsourcing Guidelines Amendments, Circular No. 899, Series of 2016
BSP Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions	BSP: IT Guidelines, Circular No. 808, Series of 2013
BSP Revised Outsourcing Framework for Banks	BSP: Outsourcing Frameworks, Circular No. 765, Series of 2012
Manual of Operation for Banks	BSP: Manual of Operation
Bank Deposits Secrecy Law	BSP: Deposits Secrecy Law, Republic Act No. 1405
Foreign Currency Deposits Act	BSP: Foreign Deposits Secrecy Law, Republic Act No. 6426
General Banking Law	BSP: Banking Law, Republic Act No. 8791
Anti-Money Laundering Act of 2001	Anti-Money Laundering Council, Republic Act No. 9160
2016 Revised Implementing Rules and Regulations Of Republic Act No. 9160, As Amended	Anti-Money Laundering Council (AMLA): AMLA Revised Implementing Rules, Republic Act No. 9160, As Amended
Credit Information System Act	Credit Information Corporation: CISA, Republic Act No. 9510
Data Privacy Act	National Privacy Commission: DPA, Republic Act No. 10173
Implementing Rules and Regulations of the Data Privacy Act of 2012	National Privacy Commission: DPA Implementing Rules, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012"
Cybercrime Prevention Act of 2012	National Bureau of Investigation, and Philippine National Police: CPA, Republic Act No. 10175
Implementing Rules and Regulations of Republic Act No. 10175	National Bureau of Investigation, and Philippine National Police: CPA Implementing Rules, Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"

E. Summary of the key requirements

Requirements and Summary	Citation
1. Due diligence Before selecting a CSP, the FSI must perform appropriate due diligence. BSFIs should ensure effective oversight processes are in place to monitor activities of third party service providers (TPSPs). BSFIs should also properly assess cyber-risk exposures from TPSPs in order to proactively adjust their cyber-risk management programs.	Outsourcing Guidelines Amendments, Section X162.4(b) BSP Information Security Guidelines, Section 2d, Annex "A": Section 3.3.3.8.4
2. 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. Banks are expected to develop acceptable performance metrics to assess outsourcing contracts and also maintain records of all outsourcing activities, which should be regularly updated and reviewed.	Outsourcing Guidelines Amendments, Section X162.4(c) BSP IT Guidelines page 12 Outsourcing Guidelines Amendments, Page 3
3. 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. If the FSI does not have the requisite technical audit expertise, the non-technical audit methods can provide minimum coverage and should be supplemented with comprehensive external IT audits. CSPs must allow BSP's internal and external auditors to review the operations and controls of the CSP as they relate to the outsourced activity. BSP should have accessibility to the CSP to audit and verify the existence and effectiveness of internal and security controls set out in the Cloud Agreement.	BSP IT Guidelines Appendix 75e, Section 5 and Annex A
4. 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 implement adequate measures to ensure that CSPs are only given access to the information and systems that they need in order to perform their function. 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. Personal data breaches must be reported to the National Privacy Commission and affected data subjects within 72 hours from the discovery of a reportable personal data breach.	Deposits Secrecy Law, Foreign Deposits Secrecy Law, General Banking Law, Credit Information Law BSP IT Guidelines Appendix 75e, Annex A DPA Implementing Rules, Section 38
5. 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. FSIs must establish, maintain, and regularly test business continuity and contingency plans for situations where the service provider cannot deliver the required services. The contingency plan must indicate whether the FSI will use another service provider or the activity will be brought back in-house. This plan should consider the costs, time, and resources that would be involved.	BSP IT Guidelines Appendix 75e, Annex A Outsourcing Guidelines Amendments, Page 3
6. Data location	BSP IT Guidelines Appendix 75e, Annex A

Requirements and Summary	Citation
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. Offshore outsourcing of a bank's domestic operations is permitted only when the CSP operates in jurisdictions which uphold confidentiality. When the CSP is located in other countries, the bank should take into account and closely monitor, on a continuing basis, government policies and other conditions in countries where the CSP is based as part of its risk assessment processes.	Outsourcing Guidelines Amendments, Page 4
7. Data use FSIs must retain exclusive ownership over all their Data and the CSP must not be able to use the Data for its own purposes.	BSP IT Guidelines Appendix 75e, Annex A.
8. 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 such as access controls or external audits and security certifications.	BSP IT Guidelines Appendix 75e, Annex A
9. 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
10. Termination FSIs must have the right to terminate the Cloud Contract by contractual notice if the BSP requires FSIs to terminate the Cloud Contract. The BSP also suggests that the Service Level Agreement, which formalises 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 may require FSIs to terminate, modify, make alternative outsourcing arrangements, if confidentiality of customer information is at risk or if BSP is no longer able to carry out its supervision functions.	BSP Outsourcing Frameworks, Appendix BSP IT Guidelines Appendix 75e, Section 3.4 and Annex A Outsourcing Guidelines Amendments, Page 5

SINGAPORE

A. 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 Info-communications Media Development Authority of Singapore (www.imda.gov.sg) ("**IMDA**"), a statutory board of the Singapore government, is responsible for the development and growth of the infocomm media industry

B. Introduction and Update

The MAS has been a proponent of cloud adoption and more broadly, of technological innovation among FSIs. July 2016 marked a turning point in the financial services sector's perception of Cloud Services, when the MAS updated its Guidelines on Outsourcing. The new guidelines provided insight into MAS' view on cloud computing for the first time, giving clarity on MAS' positive posture towards FSIs' use of Cloud Services, by recognising the benefits of the cloud. This dispelled a common misconception among Singapore's FSIs that MAS did not approve of the use of cloud, which had been a key blocker to cloud adoption.[62]

The updated guidelines were also able to reduce compliance barriers to cloud adoption for FSIs by simplifying the administrative procedure of cloud outsourcing. This entailed the removal of two regulatory requirements: the expectation that FSIs should pre-notify MAS of all "material outsourcing" arrangements,[63] and the need for FSIs to respond to a detailed questionnaire before engaging in any "significant" IT outsourcing agreement. The Technology Outsourcing Questionnaire had become a heavy administrative burden for both FSIs and CSPs alike and was not ideal for FSIs' cloud adoption given the rising complexity of cloud outsourcing arrangements.

In October 2017, MAS also released its industry transformation map (ITM) for financial services,[64] which included an agenda for continuous innovation and technology adoption, solidifying the basis for cloud adoption by FSIs.

During the Singapore FinTech Festival in November 2017, MAS revealed that it would be conducting its upcoming review of the TRM Guidelines together with industry body, the Association of Banks in Singapore (ABS).[65] This would be the first time the MAS is conducting the review alongside industry and is a positive sign that the private sector has a place in shaping FSI regulation in Singapore. Industry involvement would help MAS better recognise and tackle any regulatory obstacles to technological implementation, and expedite the process of adopting cutting-edge technologies in the financial services sector.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes.**
2. Are there specific regulations dealing exclusively with Cloud Services?	**No.** However, the MAS addresses Cloud Services in its Guidelines on Outsourcing, clearly identifying Cloud Services as a form of outsourcing and emphasising that it is regulated as per all other outsourcing arrangements.

[62] https://ncmedia.azureedge.net/ncmedia/2016/06/Cloud-in-Banking-Whitepaper.pdf
[63] http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines%20Jul%202016_FAQ.pdf
[64] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/Roadmap-for-a-Leading-Global-Financial-Centre-in-Asia.aspx
[65] http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2017/Singapore-FinTech-Journey-2.aspx

3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.
4. Is regulatory approval required?	**No**. There is no requirement for approval.
5. Is there a process to follow? If so what is the process and is there a specific form/ questionnaire to be completed?	**No.** However, FSIs are required to maintain a register of all outsourcing arrangements, and submit this to MAS at least annually, or upon request.
6. Are there specific contractual requirements that must be adopted?	**Yes.** The MAS Guidelines on Outsourcing contain a list of provisions that should be covered, at the minimum, in all Cloud Contracts. See the table below for some examples.
7. Other information/ developments	In 2013, the IDA (now IMDA) 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.

D. Relevant Regulations

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
Banking Act (Section 47)	MAS: Banking Act, Act 41 of 1970
Securities and Futures Act (Section 21)	MAS: Securities & Futures Act, Act 42 of 2001
Notice 634 Banking Secrecy - Conditions for Outsourcing	MAS: Banking Secrecy Notice, MAS 634
Technology Risk Management Guidelines	MAS: TRM Guidelines
Notice on Technology Risk Management	MAS: TRM Notice, Notice No. CMG-N02
Guidelines on Outsourcing	MAS: Outsourcing Guidelines, N/A
Business Continuity Management Guidelines	MAS: BCM Guidelines
Cloud Outage Incident Response Guidelines	IMDA: COIR Guidelines
Personal Data Protection Act	PDPC: PDPA, No. 26 of 2012

E. Summary of the key requirements

Requirements and Summary	Citation
1. Due diligence FSIs must carry out 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, Paragraphs 5.3 and 5.4 TRM Guidelines Paragraphs 5.1 and 5.2
2. Review, monitoring and control FSIs must establish a structure to manage and control the CSP according to the materiality and complexity of the outsourcing arrangement. The MAS lists six baseline measures (including creating reporting policies and procedures and conducting annual reviews) FSIs should follow to ensure that CSPs uphold performance, operational, internal control and risk management standards throughout the duration of the Cloud Contract. The Cloud Contract should include clauses to address such arrangements.	Outsourcing Guidelines, Paragraph 5.8 TRM Guidelines, Paragraph 5.1
3. Audit	Outsourcing Guidelines, Paragraph 5.9

Requirements and Summary	Citation
CSPs involved in material outsourcing arrangements must comply with any request from the MAS or the FSI to submit reports on their security and control environment. Material outsourcing arrangements should include clauses that allow the FSI to conduct audits on the CSP and its subcontractors, whether by its internal or external auditors. Additional contractual inspection rights in favour of MAS or the FSI are also required to be included in the contract. Such inspections may be performed by the FSI's internal or external auditors, the CSP's external auditors or by agents appointed by the FSI.	
4. 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' TRM Guidelines. CSPs must maintain robust security measures and comprehensive security policies. CSPs must disclose to the FSI any breach of confidentiality that involves customer information. The agreement for cloud services should state, among other things, the responsibilities of the parties to ensure the adequacy and effectiveness of security policies and practices, the party liable for losses in the event of a breach of security or confidentiality and access to and disclosure of customer information by the CSP.	Outsourcing Guidelines, Paragraph 5.6 TRM Guidelines 4.02, 5.14, 9.0.2 PDPA, Section 24
5. 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.	Outsourcing Guidelines, Paragraph 5.7 BCM Guidelines TRM Guidelines
6. Data location There is 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 ensure that the social, economic, legal and political conditions that a foreign CSP may be exposed to do not impede on the CSP's ability to fulfil its obligations stated in the Cloud Contract. FSIs should also actively address any such risks.	PDPA, Section 26 Outsourcing Guidelines, Paragraphs 5.10
7. 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 5.6.2 PDPA, Section 18
8. Data segregation FSI Customer Data must be segregated from other Data held by the CSPs by using robust physical or logical controls. 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 6.7 TRM Guidelines, Paragraphs 6.2.5 and 7.2.2
9. Subcontracting Sub-contracting should not affect the FSI's ability to monitor and control its outsourcing arrangements, and the CSP will be liable for its sub-contractors. The use of sub-contractors in any part of a material outsourcing arrangement must first be subject to FSI approval.	Outsourcing Guidelines, Paragraph 5.5.2
10. Termination The Cloud Contract should contain appropriate exit provisions, as well as the minimum period for executing an exit provision. On termination, the CSP must permanently delete, destroy or render unusable all FSI Data or the FSI must have the contractual power and means to promptly remove or destroy data on the CSP's systems.	Outsourcing Guidelines, Paragraphs 5.5.2 and 5.7.2 TRM Guidelines, Paragraph 5.2.4 PDPA, Section 25

Case Study:

Singapore's DBS Bank

DBS is a leading financial services group in Asia, with over 280 branches across 18 markets. Headquartered and listed in Singapore, DBS has a growing presence in the three key Asian axes of growth: Greater China, Southeast Asia and South Asia. DBS is at the forefront of leveraging digital technology to shape the future of banking, and was named "World's Best Digital Bank" by Euromoney in 2016.

Enabling an organisation-wide digital transformation

Since 2009, DBS has made significant investments in strategic technology initiatives to make banking more efficient and create a seamless experience for customers. This includes initiating a comprehensive re-architecture of the bank's technology, as well as catalysing a change in culture within the bank to one that is more "fintech-like" in nature. One of the core components includes leveraging cloud technology, which allows DBS to be better able to experiment in a digital way as well as deliver new applications rapidly, while adhering to the highest standards of security.

DBS has been an early adopter of cloud among FSIs, and intends to move up to 50% of its compute workload to the cloud by 2018 to support its digital transformation strategy. In the new program, AWS technical experts will work alongside DBS employees on selected technology innovation projects covering the areas of security, artificial intelligence and data analytics.

Achieving flexibility, cost savings and increased resilience

One of the first units to use AWS cloud is in DBS' Treasury and Markets (T&M) business. The bank will leverage AWS for the purpose of pricing and valuing financial instruments for risk management as this requires extensive computing power.

The cloud provides the flexibility to rapidly scale the capacity of its computing grid up or down, without having to make provisions for permanent overcapacity. In the T&M case, it will allow the bank to have a quick and yet cost-effective way of handling short term surges in trading volumes.

The bank envisages extending its cloud computing usage over time, and may shift up to 50% of its compute workload to cloud within a two-year period. This will result in dramatic cost savings, increased resilience and the ability to rapidly respond to customer demand.

Source: Thanks to AWS and DBS for providing this case study. For more information, visit https://aws.amazon.com/solutions/case-studies/dbs-bank/

SOUTH KOREA

A. Who are the relevant Regulators?

- The Financial Services Commission (www.fsc.go.kr, 금융위원회) ("**FSC**")
- The Financial Supervisory Services (www.fss.or.kr, 금융감독원) ("**FSS**")
- The Ministry of Science and ICT (www.msip.go.kr, 과학 및 정보 통신부) ("**MSIT**")
- The Personal Information Protection Commission (www.pipc.go.kr, 개인정보보호위원회) ("**PIPC**")
- The Korea Communications Commission (www.kcc.go.kr, 방송통신위원회) ("**KCC**")

B. Introduction and Update

The Korean National Assembly passed the world's first Cloud Computing Act in March 2015, which allowed the public sector to adopt Cloud Services upon obtaining the Korea Internet and Security Agency (KISA)'s certification. Prior to the Act, data security concerns prohibited the move to cloud by government services.[66] The Cloud Computing Act encourages public institutions to prioritise the use of cloud to become more cost-effective, stay competitive and improve operational efficiency, indicating the Korean government's pro-cloud stance. However, the stringent requirements of the KISA certification – including physical network separation, data localisation, and local algorithm use, has slowed the availability of Cloud Services in the country.[67] At the point of writing, just five local CSPs had received the cloud security certification required to provide cloud services to the public sector, illustrating the challenging regulatory environment facing international CSPs.[68]

South Korea has released further statements clarifying Cloud Services use in the financial sector:

- The FSS released a statement in January 2018 with details on its position on Financial Companies' Use of Cloud Computing, providing an update on the number of financial companies adopting cloud and highlighting a number of use cases of cloud adoption such as internal business processing and information investment analysis.[69]
- MSIT and the KISA also recently announced their plans to collaborate on developing a conducive security and regulatory environment for the development and usage of cloud technologies in sectors which require high levels of information security, such as the medical and finance sectors.[70]
- In October 2016, the Financial Security Institute (FSI) released "Guidelines on the Use of Cloud Services in the Financial Industry", as per which finance companies can adopt cloud computing, but only for non-critical processing systems, which excludes the use of cloud technologies for systems handling unique identification information and personal credit information.
- This follows an announcement by the FSS and FSC on South Korea's outsourcing guidelines for FSIs in June 2015, which aimed to ease the regulatory burden on FSIs' when outsourcing data processing functions, including cloud computing technologies[71]. However, while FSIs

[66] http://www.asiacloudcomputing.org/images/documents/cri2016_acca.pdf
[67] https://aws.amazon.com/blogs/security/amazon-web-services-is-the-first-global-cloud-service-provider-to-achieve-the-korea-information-security-management-system-certification/
[68] https://isms.kisa.or.kr/main/csap/issue/?certificationMode=list
[69] http://www.fss.or.kr/fss/kr/promo/bodobbs_view.jsp?seqno=21018&no=13537&s_title=&s_kind=&page=1
[70] http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1373326
[71] http://www.fsc.go.kr/eng/new_press/releases.jsp?menu=01&bbsid=BBS0048&selYear=2015#31027

are now allowed to engage CSPs whose data hosting infrastructure is located outside of South Korea, this is only for less-significant workloads.

Other recent developments in South Korea are telling of its support for broader development in the IT sector and fintech industry. In January 2018, the Korean government identified fintech as a new and important technology for the fourth industrial revolution.[72] The government plans to ease rules governing financial institutions through a fintech regulatory sandbox, an action plan for which was scheduled to be announced in February 2018. In addition, the government has earmarked KRW 2 trillion (USD 1.87 billion) to develop the fintech sector and support big data use between 2018 and 2019. South Korea has also allocated a total of KRW 5.8 trillion (USD 5.3 billion) to develop its IT sector in 2018, paving its way into the fourth industrial revolution.[73] Big data, the Internet of Things (IoT), information security, and cloud computing, among others, will be key areas of focus.

C. Overview

1. Is the use of Cloud Services permitted?	**Yes, but for less-significant information processing systems only.** See "Is regulatory approval required?"
2. Are there specific regulations dealing exclusively with Cloud Services?	**Yes.** In October 2016, the Financial Security Institute (FSI) released its "Guideline on Use of Cloud Services in Financial Industry" and in March 2015, the Korean National Assembly passed the Act on the Development of Cloud Computing and Protection of Users (The "Cloud Computing Act").
3. Are there other regulations/ guidelines that are relevant?	**Yes.** See next Section.
4. Is regulatory approval required?	**Yes.** As per the "Revision to the Regulation on Financial Institutions Outsourcing of Data Processing Business & IT Facilities" in June 2015, approval prior to outsourcing of less-significant information systems is not required, instead FSIs can report the outsourcing to the FSS after the event. However, as per the "Regulation on Supervision of Electronic Financial Transactions", in order to use Cloud Services provided by a third party, an FSI is required to designate less-significant information processing systems and submit a report to the FSS within seven days from the date of designation. The report must contain the evaluation standards for importance of information assets, result of designation, and management plans, and the FSS in response can ask the FSI for improvement and supplementation if the initial report is deemed inappropriate. The Financial Security Institute's October 2016 Guideline presents standards for designation of less-significant information processing systems that have less impact on the safety of electronic financial transactions. Systems that process unique identifiable information or personal credit information cannot be designated as less-significant information processing systems.
5. Is there a process to follow? If so what is the process and is there a specific form/ questionnaire to be completed?	**Yes.** To use the cloud for less-significant information processing systems, FSIs are required to send a designation report to the FSS within seven days of designating the less-significant information processing systems. In response, the FSS can ask for improvement to the initial report, if it is deemed insufficient. To use Cloud Services without designating the outsourced services as less-significant information processing systems, FSIs must fully comply with the "Regulation on Supervision of Electronic Financial Transactions", which requires physical separation of information processing systems from any external communication network. In

[72] http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=&sword=&r_url=&menu=7210100&no=32275
[73] http://msip.go.kr/SYNAP/skin/doc.html?fn=c13976160ocf6dfef2a13a68d75369db&rs=/SYNAP/sn3hcv/result/201711/

	addition, any data containing significant information such as personally identifiable information must remain in local data servers, and systems processing "identifiable financial information of individuals" cannot be designated as a "less-significant information processing" system and therefore may not be outsourced.
6. Are there specific contractual requirements that must be adopted?	**No.** FSIs will no longer be required to sign the standard form contract when contracting with CSPs, as long as the contract includes the regulatory requirements (e.g. obligations to permit the regulator to supervise and inspect the CSP).
7. Other information/ developments	In March 2015, the Korean National Assembly enacted the Act on Promotion of Cloud Computing and User Protection (The "Cloud Computing Act"), the proposal for which was submitted on 16th October 2013. The Act permits the use of Cloud Services by public institutions, which was previously not allowed. In anticipation of an increase in the use of cloud computing due to the enactment of the Cloud Act, MSIT established and announced the "Information Protection Measures for Vitalization of Cloud Services" on September 9, 2015. Below are some tasks the Ministry plans to undertake: • Prepare and implement standards for cloud information protection including administrative and technical measures that cloud enterprisers must comply with in order to protect information. • Establish and operate a cloud information-sharing analytical centre as a prevention system for cloud infringement accidents.

D. Relevant Regulations

Full Title	Regulator, Abbreviated Title, and Citation/ Reference
Amendment of Regulations on the Business Entrustment of Financial Institutions	FSC/FSS: Business Entrustment Regulation, FSC Press Release, November 13, 2017
The Act on the Development of Cloud Computing and Protection of Users	MSIT: The Cloud Computing Act, [Enforcement Date 26. Jul, 2017.] [No. 14839, 26. Jul, 2017., Amended by Other Act]
Regulation on Supervision of Electronic Financial Transactions	FSC/FSS: Electronic Financial Transactions Regulation FSC Public Notice No. 2016-24, Jun. 30, 2016
The Act on Promotion of Information Communication Network Utilisation & Data Protection	KCC: The Information & Communication Network Act, Act No. 11322 (Feb. 17, 2012)
Banking Act	FSC/FSS: BA, Act No. 9784 (Jun. 9, 2009)
Insurance Business Act	FSC/FSS: IBA, Act No. 8902 (Mar. 14, 2008)
Regulation on Business Delegation of Financial Institutions	FSC/FSS: The Regulations, FSC 2005-39
Revision to Regulation on Financial Institutions' Outsourcing of Data Processing Business & IT Facilities	FSC/FSS: Outsourcing Regulation Revision, FSC Press Release June 9, 2015
Regulation on Outsourcing of Data Processing and Computer Facilities of Financial Companies	FSC/FSS: June Regulation, FSC Official Announcement No. 2013-17
The Personal Information Protection Act	PIPC: PIPA, Act No. 11690 (2013.3.23)
FSI Guidelines on Use of Cloud Services in the Financial Industry	FSI Cloud Guidelines

E. Summary of the key requirements

Requirements and Summary	Citation
1. Due diligence	The Regulations, Appendix 2

Requirements and Summary	Citation
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.	
2. Review, monitoring and control FSIs must establish a procedure to monitor the financial position of CSPs, risks, emergency measures and test results for these emergency measures.	The Regulations, Appendix 2
3. Audit The FSI must ensure that the FSC and the FSS have the ability to access and audit the CSP. The FSI must also have a right to audit the CSP.	The Regulations, Appendix 2 The June Regulation, Article 8-1 and Table 1
4. 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 failures and data leakages.	The Regulations, Appendix 2 The June Regulation, Article 5-1 The Cloud Computing Act, Article 25
5. 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, e.g. having in place back-up procedures to secure continuity of the service.	The Regulations, Appendix 2
6. Data location The use of offshore data centres by FSIs is allowed.	Outsourcing Regulation Revision (FSC Press Release June 09, 2015)
7. Data use The CSP must not be allowed to use the Data for any other purpose beyond providing the services to the FSI. CSPs must not disclose personal customer data to a third party without prior consent. A failure to get consent prior to using or disclosing customer information to a third party, will result in penalties in the form of imprisonment or fines.	The June Regulation, Article 4-5 The Cloud Computing Act, Article 34
8. Data segregation The CSP must separately manage the FSI's information, granting access only to authorised persons. To use Cloud Services without designation of less-critical information processing systems, FSIs are required to physically separate their network from external communication networks. For less-significant information processing systems located in the external network of a CSP, a financial company shall separate such systems from other institutions' networks using the same cloud. For less-significant information processing systems located in the internal network of a CSP, a financial company shall separate such systems from any external networks and outside institutions' networks using the same cloud.	The Regulations, Appendix 2 Regulation on Supervision of Electronic Financial Transactions, Article 15 FSI Cloud Guidelines, Chapter 4
9. 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.	The Regulations, Appendix 2 The June Regulation, Article 4-4
10. Termination If a CSP intends to terminate a business, it must notify the user of the termination and return the user information before the end of the business, and destroy the user information held.	The Cloud Computing Act, Article 27

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.

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

"Customer" means a customer of an FSI, such a 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.

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

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

"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 identifiable 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 with the FSI, either as a Customer of or a staff member.

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

"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.

The ACCA is a leading industry association comprising the stakeholders of the cloud computing ecosystem in Asia. The ACCA works to ensure that the interests of the cloud computing community are effectively represented in the public policy debate.

Our primary mission is to accelerate the growth of the cloud market in Asia, where we promote the growth and development of cloud computing in Asia Pacific through dialogue, training, and public education.

Through regular meetings, we also provide a platform for members to discuss implementation and growth strategies, share ideas, and establish policies and best practices relating to the cloud computing ecosystem.

ACCA Member Companies

ADN Telecom
aws
CISCO
DIGITAL REALTY
EQUINIX
ERICSSON
Globe Business
Google
Microsoft
salesforce
TrustSphere Because Relationships Matter
verizon

Join us as a member today!

secretariat@asiacloudcomputing.org
asiacloudcomputing.org
is.gd/accacloud
@accacloud