asia cloud computing association

Better on the Cloud

Financial Services in Asia Pacific

2021

ACKNOWLEDGEMENTS: Support for this publication was generously provided by Gold sponsor Google Cloud, Silver sponsor HSBC Ltd, and Bronze sponsor AWS, with the research assistance of TRPC Pte Ltd. The ACCA is committed to independent, quality research, and the conclusions of this report are not determined or influenced by sponsorship.

The ACCA would like to acknowledge the following individuals for their contributions:
Project Manager: Stacy Baird, TRPC Pte Ltd.
Lim May-Ann and Hiromi Oka, Asia Cloud Computing Association
Yam Ki Chan, Google Cloud
Bojan Obradovic, Daniel Warelis, HSBC Ltd.
Agne Makauskaite, Amazon Web Services
Researchers: Faiza Saleem, Cheryl Tan, Jenny Wan, TRPC Pte Ltd.
Cover image credits: Christian Wiediger, https://unsplash.com/photos/32RQSc3cRxQ

The ACCA is the apex industry association representing the stakeholders of the cloud computing ecosystem in the Asia-Pacific (APAC) region. Our mission is to accelerate adoption of cloud computing in APAC by creating a trusted and compelling market environment and a safe and consistent regulatory environment for cloud computing products and services. The association works to ensure that the interests of the cloud computing community are effectively represented in the public policy debate. Drawing on subject-matter expertise from member companies, expert working groups, and special interest groups, it develops best practice recommendations and other thought leadership materials.

To find out more on how to join us, email secretariat@asiacloudcomputing.org, or visit our website at www.asiacloudcomputing.org

asia cloud computing association

Better on the Cloud: Financial Services in Asia Pacific 2021

Table of Contents

Executive Summary - Better on the Cloud: Financial Services in Asia Pacific 2021

The Asia Cloud Computing Association (ACCA) started reporting on the state of the marketplace for Financial Institution (FI) adoption of cloud computing in 2015. Since then, adoption of cloud by FIs has accelerated, particularly amid the COVID-19 crisis. This 2021 report updates our earlier analysis and recommendations with these developments in mind, noting the benefits that have been accrued by jurisdictions that facilitated greater cloud adoption. We hope to encourage all regulators to pursue policies that enable FIs to adopt cloud services. This would facilitate greater consistency in cloud related policies across the region, allowing for the benefits seen thus far from cloud adoption to expand exponentially.

Since our last report, the ACCA has been encouraged by the efforts of leading regulators to embrace the use of cloud by FIs. Regulators are increasingly working with FIs and cloud service providers (CSPs) to better understand how cloud is a key support technology for FI business objectives (including risk management). In many cases, they have been working to update, adapt, and revise regulations and guidelines to enable FI adoption of cloud computing technologies. These are positive developments that we feel demonstrate the importance and benefit of continued dialogue between regulators, FIs and CSPs. The ACCA is encouraged to see that many regulators are now embracing the use of cloud by FIs. We would like to see the regulators in more markets take a similarly favorable approach to FI adoption of cloud.

Throughout this report, we will use the term "cloud" to describe public cloud, unless otherwise noted. It should be noted that this report only examines regulations related to the banking subsector and is not inclusive of insurance or securities regulations.[1]

Accelerated adoption of cloud in the FSI

Since the last update to this report in 2018, there has been a substantial acceleration in the adoption of cloud services by FIs, and regulators are demonstrating more support for this dynamic. Traditional FIs have been more aggressive in their adoption of cloud as they seek to transform their businesses through new customer offerings empowered by data analytics, artificial intelligence, and advanced back-office digitalization. In addition, new FI entrants such as Virtual Banks are "born in the cloud", with their entire operations based on cloud computing technologies. The industry is in a period of rapid innovation that is enabled by cloud computing.

According to the business intelligence firm International Data Corporation (IDC), FIs that had begun their digital transformation having invested in technology such as cloud, open Application Programming Interface (API) architecture, Artificial Intelligence (AI), security and mobility prior to the impact of COVID-19, will do better through the crisis and recover more quickly.[2] There is evidence that this is already happening in Asia much faster than in the North America or Europe, Middle East and Africa (EMEA) markets, due to a speedier recovery

1 Please note that this report only reviews the banking sector of the financial industry (as in our 2015 and 2018 reports.) We use the term FI generally when discussing an entity in the abstract ('An FI may find the regulation restrictive.'. We use 'bank' when referring to a specific bank (National Bank), or banking regulations (In the market profiles) or when describing a term of art, such as 'virtual bank' or 'digital banking'.
2 IDC, 2020, Crisis is Accelerating Digital Transformation in Banking, Again, https://inthecloud.withgoogle.com/idc-financial-services-digital-transformation-20/dl-cd.html.

from the COVID-19 crisis.[3] In Asia, enterprise leaders already see themselves in the "next normal" and are focused on the future of the enterprise, having largely recovered from the economic challenges created by the pandemic.

FIs are also experiencing competition from new non-traditional FIs and businesses. Financial Technology (FinTech) start-ups are identifying unmet consumer needs and building products and services on the cloud to meet those needs. Traditional FIs are also developing new cloud-facilitated products and services to meet this competition head-on.

The New Normal

Cloud adoption has been accelerated, with FIs forced to quickly adjust to changing circumstances as a result of the COVID-19 crisis; furthermore, lessons from the experience have further fuelled their digital transformation. As demonstrated in the COVID-19 crisis, FIs responded quickly and successfully, without disruption to changes in the financial services environment. That FI resilience has been supported and enhanced by the availability of cloud computing.

The response to the COVID-19 pandemic has proven that employees with the flexibility to work remotely can do so productively and collaboratively. FI customers can transact business online or in apps. In addition, activities that were previously paper-based, such as identity verification and other Know Your Customer (KYC) requirements, can now be conducted confidentially without an in-person exchange, provided the regulatory environment supports remote verification.

Cloud has also increased the ability of FIs to transfer an increasing amount of financial services activity – both customer-facing and back-office operations – to the online environment. New approaches are being introduced so that managers are able to maintain relationships with and oversight of remote employees, as well as for employees to interact with one another, balancing limited physical interactions with predominantly virtual connections.

This rapid shift to a digital environment will become the new normal, as employees and customers alike have rapidly come to appreciate personal efficiency, both in terms of time savings and the ease of interactions and transactions. As FIs continue to improve their business operations through more efficient, effective processes, meaningful collaboration, better data analysis and risk management, and improved compliance will continue to drive further acceptance of cloud across their functions.

Cloud can improve resilience and business continuity management

As described in the PWC report, Financial Services 2020 and Beyond: Embracing Disruption, FI CEOs expect "substantial growth in the use of public cloud."[4] Cloud will contribute to greater, more agile growth in services, better resilience, improved compliance and, as evidenced by the COVID-19 crisis, enhance the ability of businesses to adjust to changing market conditions.

---

3 IDC's COVID-19's Impact on IT Spending Survey evidenced the 'Progress of Recovery and Transformation Acceleration in Banking by Region'. With the question asked: 'Of the following choices, which one best describes where your organization currently is?' The results were notable. In this self-evaluation at an enterprise level, Asia is well ahead of other regions along the continuum of crisis to recovery to new normal, with 59% of respondents describing themselves as having a business focus on the future of the enterprise, and already in the 'next normal,' while North America, 33% of respondents characterized their focus on business continuity in the economic situation of the COVID-19 crisis, and 55% focused on cost optimization/in economic slowdown. In EMEA, the 48% of respondents viewed themselves in cost optimization/economic slowdown and 22% focused on business resiliency with the economic situation of a recession. IDC, COVID-19 Impact on IT Spending Survey, July 2020, cited in IDC, 2020, Crisis is Accelerating Digital Transformation in Banking, Again. https://inthecloud.withgoogle.com/idc-financial-services-digital-transformation-20/dl-cd.html.

4 PWC, 2020, Financial Services Technology 2020 and Beyond: Embracing Disruption, https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf.

The following outlines some of the established benefits from cloud usage in financial services. It can:

1. Significantly improve the resilience of FIs and enable them, their employees and customers across the globe to securely do business. This enables FIs to pivot to remote working more easily, quickly upgrade customer-facing software, and address fraud;[5]
2. Enable FIs to break their data out of the organizational structures that legacy systems helped create, serving as an alternative to fragmented legacy ID and reducing the overall cost of IT ownership;[6]
3. Improve business processes by enabling rapid scaling of automation, faster access to data, more sophisticated and granular data analytics, improving decision-making;[7]
4. Accelerate and enhance financial inclusion for small businesses and low-and moderate-income consumers, by improving risk analysis[8] for account opening and loans;
5. Facilitate Digital Banking, including mobile payments and online banking, to meet many consumers' and financial services' needs and, importantly, improve access to financial services, thereby bringing more citizens into the economy[9];
6. Enable financial services to rapidly develop and expand online services to customers 24/7, minimizing trips to the bank;[10]
7. Cloud has enabled FIs to adjust workflows to better manage government benefits programs online. [11] Successful stimulus programs will need deployment and accountability through financial institutions, and cloud facilitates that process;
8. Help FIs, through greater use of Artificial Intelligence (AI), to improve their efforts to fight against financial crime, enhance Regulatory Technology (RegTech) capabilities, better manage spikes in customer service demand and relieve dependency on physical branches; and
9. Enable Open Banking by providing the capabilities needed for meeting unpredictable customer demand, as well as managing an advanced, interconnected API system.

Recommendations

As a result of increased adoption of cloud and a greater awareness of its capabilities, we have revised several recommendations and added two that will enable regulators to further accelerate digital transformation in financial services, while mitigating associated risks.

The first is that the regulator has affirmed the adoption of cloud for FIs, which provides FIs with the support they may need to make that switch. Thus, we are looking to see if the regulator, rather than merely accepting FI cloud adoption, is now affirmatively encouraging FIs to consider the benefits of cloud.

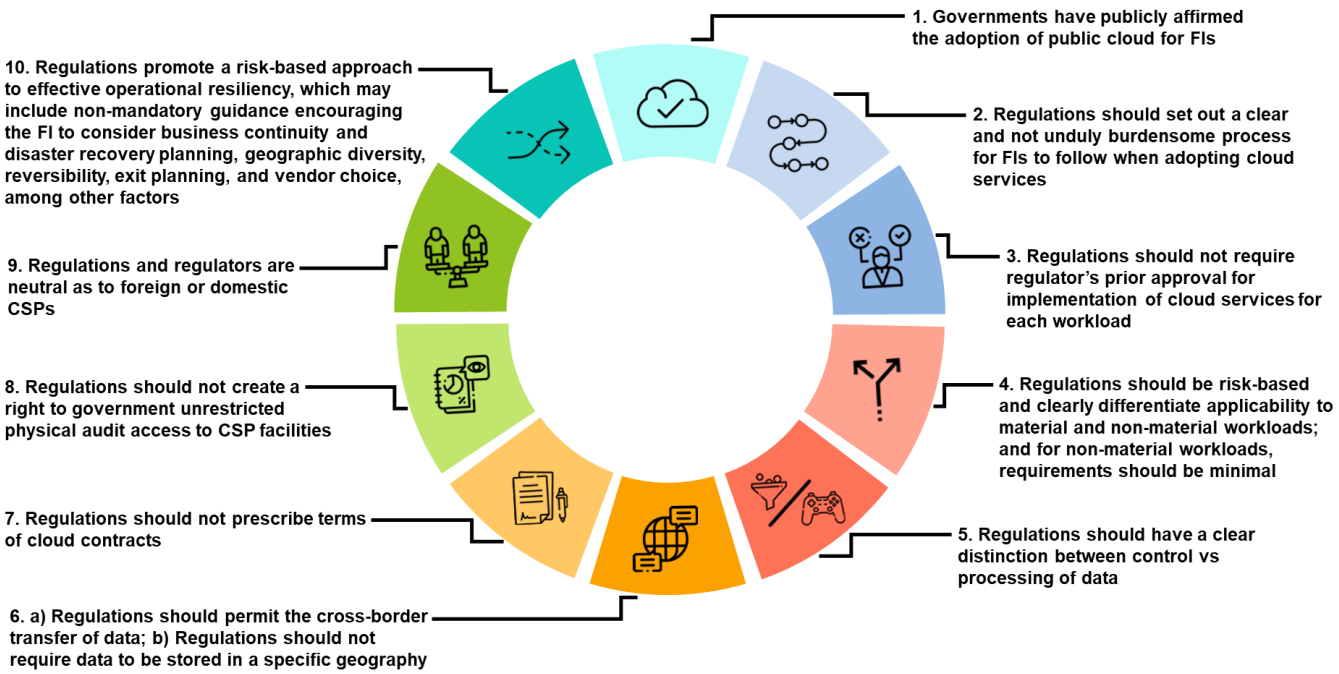
The second new recommendation encourages regulators to promote a risk-based approach to operational resiliency, which may include non-mandatory, non-prescriptive guidance to FIs to consider cloud as a favorable part of risk management, including consideration of Business

5 CapGemini, 2020, COVID-19 Conversations: Cloud Computing, https://www.capgemini.com/gb-en/2020/11/covid-19-conversations-cloud-computing/.
6 PWC, 2020, Financial Services Technology 2020 and Beyond: Embracing Disruption, https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf.
7 McKinsey, 2020, Three Actions CEOs can take to get value from Cloud Computing, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/three-actions-ceos-can-take-to-get-value-from-cloud-computing.
8 Experian, 2020, How Cloud Computing Will Drive Financial Inclusion, https://www.experian.com/blogs/insights/2020/11/how-cloud-computing-will-drive-financial-inclusion/.
9 Forbes, 2020, COVID-19 Sways Banks To Adopt Cloud, But They Will Need A Strategy Before Diving In https://www.forbes.com/sites/alanmcintyre/2020/09/28/covid-19-sways-banks-to-adopt-cloud-but-they-will-need-a-strategy-before-diving-in.
10 CapGemini, 2020, COVID-19 Conversations: Cloud Computing, https://www.capgemini.com/gb-en/2020/11/covid-19-conversations-cloud-computing/.
11 Forbes, 2020, COVID-19 Sways Banks To Adopt Cloud, But They Will Need A Strategy Before Diving In https://www.forbes.com/sites/alanmcintyre/2020/09/28/covid-19-sways-banks-to-adopt-cloud-but-they-will-need-a-strategy-before-diving-in.

Continuity and Disaster Recovery Management (BCM/DRM), geographic diversity, reversibility, exit planning and vendor choice, among other factors to address risk.

The ten recommendations are represented in Figure 1.

Figure 1: Ten Regulatory Recommendations



Source: ACCA, 2021

Conclusions

From our analysis (see Table 1), the leading markets have fully achieved most, if not all of our recommendations. FI regulators in Australia, Philippines, Singapore and Japan have made strong positive statements or, through their guidance, clearly support the adoption of cloud computing by the FSI. The laws of Japan and Singapore allow transfer of data outside the jurisdiction; their regulations do not require the regulator to give approval before an FI's move to the cloud; and regulators in these markets encourage (without mandating an FI's consideration of a CSP's data centers in geographically diverse locations, reversibility, exit planning and vendor choice, among other factors) a risk-based approach.[12]

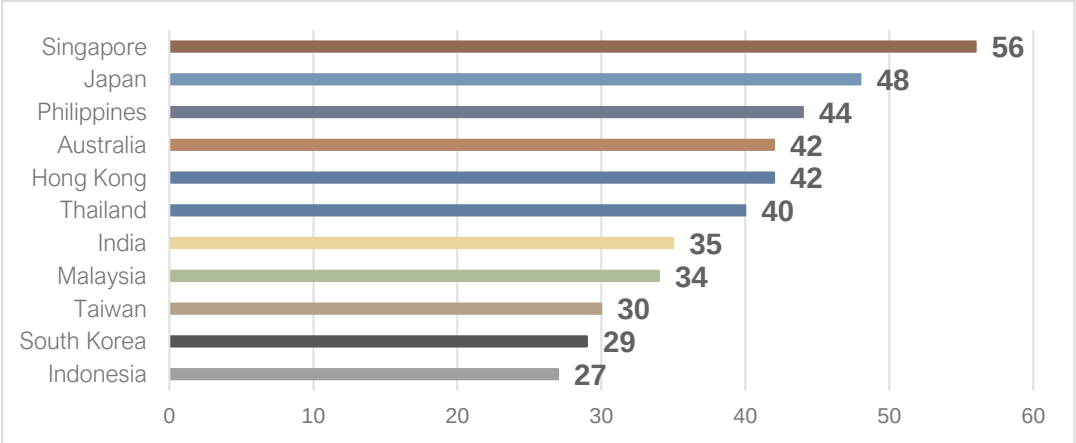
12 FSA, 2014, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf.

Table 1: Financial Services in Asia Pacific 2021: Market Scores and Ranking

REGULATORY RECOMMENDATION / MARKET & RANK	SG 1	JP 2	PH 3	AU =4	HK =4	TH 6	IN 7	MY 8	TW 9	KR 10	ID 11	UK -
1. Governments have publicly affirmed the adoption of public cloud for FIs.	6	6	6	4	2	2	4	6	2	2	6	6
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services.	6	6	4	6	4	4	4	4	4	4	4	6
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload.	6	6	0	0	0	0	4	0	2	4	0	6
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal.	6	0	2	6	2	4	2	4	6	4	0	6
5. Regulations should have a clear distinction between control vs processing of data.	2	2	2	0	6	6	4	6	0	6	4	6
6. Geographic Restrictions:												
6a. Regulations should permit the cross-border transfer of data.	3	3	3	3	3	3	1	3	1	1	1	3
6b. Regulations should not require data to be stored in a specific geography.	3	1	3	3	1	3	0	3	1	0	0	3
7. Regulations should not prescribe terms of cloud contracts.	6	6	6	6	6	6	2	2	2	2	2	6
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities.	6	6	6	2	6	6	2	0	6	0	0	6
9. Regulations and regulators are neutral as to foreign or domestic CSPs.	6	6	6	6	6	2	6	6	2	2	6	6
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.	6	6	6	6	6	4	6	0	4	4	4	6
TOTAL SCORE	**56**	**48**	**44**	**42**	**42**	**40**	**35**	**34**	**30**	**29**	**27**	**60**
MARKET	**SG**	**JP**	**PH**	**AU**	**HK**	**TH**	**IN**	**MY**	**TW**	**KR**	**ID**	**UK**

Source: ACCA, 2021

Figure 2: APAC Markets' Performance Against 10 Regulatory Recommendations



Source: ACCA, 2021

* Maximum score is 60

Beyond the leading regulators, there is a group of markets where the shift to cloud is more challenging because some regulatory requirements tend to impede cloud adoption and technological innovation in the FSI. Examples of these markets include Thailand, Malaysia, and India. There are variations on why this is the case for each of these markets, and we examine these in the detailed market analyses within the report.

- India is challenging for several reasons, including a number of geographic restrictions, and in some cases a lack of clarity often sees the FI seeking de facto regulatory approval for each workload an FI moves to the cloud.[13]
- Malaysia is challenging, as requirements are (in some cases) overly prescriptive.[14] For example, as to Recommendation 10, although the BCP focuses on a risk-based approach to resilience, it is highly detailed and prescriptive as to how an FI takes such an approach.
- Thailand requires FIs using overseas service providers to gain prior approval for material outsourcing arrangements.

Finally, there are three notable markets in which leveraging global CSP services for the FSI is currently very difficult: Taiwan, Indonesia and South Korea.

- In Taiwan, the processing and storage of FI customer data is, in principle, to be conducted within Taiwan, and FIs are required to obtain prior approval when outsourcing material cloud service operations to overseas service providers. The regulatory requirements for using global CSP services are prescriptive and the processes are relatively burdensome.
- The most challenging aspect of doing business in Indonesia is that regulations apply to all FI workloads, material and non-material, and for each time an FI moves a workload to the cloud, approval is required.[15] Use of onshore data centers is generally required, subject to exceptional approval.

13 RBI, 2010, 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf.
14 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323.
15 OJK, 2016, Regulation No. 38/POJK.03/2016, http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf.

- South Korea's regulations do not only prescribe the terms of cloud contracts between FIs and CSPs, but also require FIs to audit CSPs, including physical inspection on CSP facilities prior to each of its implementation of cloud services. Cross-border transfer of data is not permitted in cases of material workload that contains unique personal information (UPI) or personal credit information (PCI).[16]

As a point of reference, the report also examines the regulatory environments of the United Kingdom and the United States (looking at both the federal law of one key agency and the laws of New York State as illustrative). Notably, both of these major financial markets have substantially or fully embraced the digitalization of the FSI that cloud enables. Further, although we score the UK, because we look at the regulations of only one of several federal banking regulators and the regulator in only one of 50 states for contextual illustration, we do not score the US.

Mapping Cloud Adoption against Cloud Policy for FIs

A note on rankings: to give a sense of how well the financial services regulator is moving the industry toward cloud adoption, as compared to the more general public policy objectives of their government (e.g. a Cloud First policy for the public sector, encouraging broadband deployment and other factors), we have provided the ranking of the markets in this report, and for a point of reference, include on the Y-axis the ranking according to the ACCA 2020 Cloud Readiness Index.[17]

For the most part, rankings for the FSI correspond to the general cloud readiness of each market. The two outstanding markets are the Philippines and Korea, but for different reasons. The Philippines for its better performance in the FSI compared to general readiness. Korea, for the poor showing in the FSI relative to overall readiness.

16 KCC, 2018, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=50484&lang=ENG.
17 Asia Cloud Computing Association, 2020, Cloud Readiness Index 2020 https://www.slideshare.net/accacloud/the-cloud-readiness-index-cri-2020-by-the-asia-cloud-computing-association-acca.

Figure 3: Market Ranking

Source: ACCA, 2021

Accelerated FI adoption of cloud: updates since 2018

Regulators have actively worked with the financial services industry (FSI) to understand how they are adopting the use of cloud computing across various financial processes. They are increasingly working with FIs and cloud service providers (CSPs) to understand how cloud can be a key support technology for FI business objectives (including addressing risk), and, in many cases, have been working to update, adapt, and revise regulations and guidelines to enable FI adoption of cloud computing technologies. These are positive developments that we feel demonstrate the importance and benefit of continued dialogue between regulators, CSPs and FIs.

The ACCA is encouraged to see that leading regulators are now embracing the use of cloud by FIs.[18] We would like to see the regulators in more markets to take a similarly favorable approach to cloud adoption. This 2021 report updates our earlier recommendations with these developments in mind. We hope to encourage all regulators to pursue more favorable policies that enable FIs to more easily adopt cloud services and achieve greater cloud consistency in the policies across the region, improving compliance among Asia-Pacific markets.

Accelerated adoption of cloud for the FSI

Since our 2018 report, traditional FIs have accelerated their adoption of cloud as they transform their businesses through new customer offerings and advanced back office digitalization. The industry is in a period of rapid innovation, enabled by cloud computing. Key developments include:

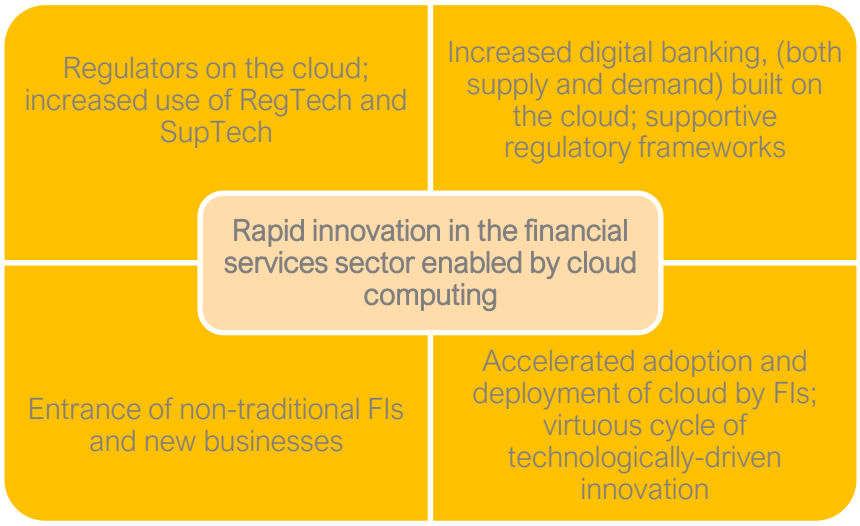
- ***Increased digital banking, built on the cloud.*** There is an increase in digital banking based on cloud services among both new market entrants and traditional banks. As the technology improves and regulator comfort levels increase, several major FIs will continue to move core business processes, products and services to the cloud in leading markets where allowed by the regulators. Hong Kong, Malaysia, and Singapore, among others in the region, have also begun to issue licenses to all-digital banks, which is part of their broader efforts to develop more inclusive access to financial services; innovation for customers; and safer, more efficient banking. These digital banks operate almost exclusively on the cloud.
- Cloud has played an important role in enabling the advancement and adoption of digital payment systems, as reliance on cash transactions has been impeded by COVID-19 restrictions. There are also new services adopting new cloud-native software as a service ("SaaS") that offer multiple functionalities needed to operate key banking components (e.g., Thought Machine's *Vault*, Mambu and Temenos).
- ***Regulators on the cloud.*** Supervisors have been exploring use cases for cloud computing in the adoption by the FSI of regulatory technology ("RegTech") and their own adoption of Supervisory Technology ("SupTech"). Both of these

18 The ACCA started reporting on the state of the marketplace for Financial Institution (FI) adoption of cloud computing in 2015. As in the past, throughout this report we will use the term 'cloud' to describe public cloud, unless otherwise noted. This report also examines only regulations related to the banking subsector and is not inclusive of insurance or the securities regulations. Please also note that this report only reviews the banking sector of the financial industry, as in our 2015 and 2018 reports. We use the term FI generally when discussing an entity in the abstract, i.e. 'An FI may find the regulation restrictive.'. We use 'bank' when referring to a specific bank (National Bank), or banking regulations (In the market profiles) or when describing a term of art, such as 'virtual bank' or 'digital banking'.

typically use cloud services in some form. For regulators, data collection, surveillance and analytics is accelerated and streamlined using artificial intelligence and machine learning built on the cloud to analyze suspicious transaction reports and detect money laundering and other forms of fraud.[19]

- The Monetary Authority of Singapore (MAS) was an early adopter, using SupTech initially to ensure data quality, and more recently to analyze suspicious transaction reports and find potential money laundering networks.[20] In the Philippines, Bangko Sentral ng Pilipinas (BSP) has partnered with the Regtech for Regulators Accelerator to develop a prototype for an API-based SupTech solution to extract regulatory reports directly from FIs.[21]
- ***Non-traditional FI and new businesses.*** Further accelerating adoption, FIs are also experiencing competition from new non-traditional FIs and businesses. FinTech start-ups are identifying unmet consumer needs and building products and services on the cloud to meet those needs. Traditional FIs are also developing new cloud-facilitated products and services to meet this competition head-on.
- Cloud services enable both the start-up and the traditional institution to develop new user experiences and offer new products and services to the market. With the elasticity of cloud services, an FI can experiment at small scale and easily scale up with wider adoption of a service or product, aligning costs with scale. Costs are moved from being a large, fixed capital expenditure to an operational expense, with granular spending control. Cloud computing also allows an FI to rapidly adapt to changing market conditions or a change in business priorities. Regulators and FIs are accelerating their use of cloud, which is transforming the industry, improving business processes and facilitating better service to customers while preserving regulatory oversight and compliance, and improving the security and resilience of their institutions.

Figure 4: Factors Contributing to Increasing Innovation in Cloud Use By FIs



Source: ACCA, 2021

19 Fintech News, October 2019. What is Suptech? An Overview of this Rapidly Growing Space, https://fintechnews.ch/regtech/what-is-suptech-an-overview/31289/
20 Bank for International Settlements, 2018, Innovative technology in financial supervision (suptech) – the experience of early users https://www.bis.org/fsi/publ/insights9.pdf.
21 Chambers and Partners, 2020, Philippines Law and Practice, https://practiceguides.chambers.com/practice-guides/fintech-2020/philippines

The COVID-19 crisis has further accelerated the digitalization of FIs

Many FIs accelerated deployment of cloud services to respond quickly to changes in the financial services environment because of the COVID-19 crisis, which shows that cloud computing can play an important role in enhancing FI resilience.

In the past, the closure of offices and branches would have created considerable difficulties for some elements of the banking population. However, the COVID-19 crisis has highlighted that employees can work remotely effectively, productively and collaboratively, while customers can transact business online or via FI apps. Moreover, paper-based activities such as identity verification can be done confidently without an in-person exchange. These are important examples of activities that are carried out in cloud-based environments.

As the period of working remotely has stretched from weeks to months, much has been learned. Cloud has contributed to FIs' ability to move more financial service activity – both customer-facing and back-office operations – to the online environment.

- Using cloud capacity, FIs can rapidly offer new services online and via mobile apps that allow customers better access to financial services without having to go into a branch office.
- FI employees suddenly finding themselves having to work remotely can securely access their office systems on a mass scale and remain productive.
- Cloud-based services facilitate meetings securely (e.g. Amazon Chime, Cisco Webex, Google Meet, Microsoft Teams and Zoom) and maintain productivity with secure suites (e.g. Amazon WorkDocs, Google Workspace and Microsoft 365).
- These cloud-based tools have enabled a rapid adoption of new ways to communicate and collaborate that have improved business efficiency and mitigated the risk of stress on the FI's IT system with capabilities that would have been far more challenging and costly without the adoption of cloud computing. New approaches are being introduced for managers to maintain relationships with and oversight of remote employees, and for employees to interact, balancing limited physical interactions with predominantly virtual connections.

In the short term, cloud has become key to allowing FIs to sustain business continuity and meet customer's needs in a challenging time where physical contact has been minimal. In the longer term, these conditions have accelerated adoption of cloud and the digitalization of business operations: more efficient, effective processes, meaningful collaboration, better data analysis and risk management and improved compliance. Indeed, with the many improvements, some have begun to describe this as the new normal.

Cloud enhances FI resilience and supports economic recovery

Although branches are closed to customers, online access has increased, including the use of cloud-based apps and web portals. New features are being developed rapidly to reduce the need for personal interactions in a branch. FIs and technology companies are developing secure digital alternatives to previously non-digital FI processes, such as in-person identity verification, physical signatures and the requirements for physical copies of documents. FIs such as DBS now allow individuals and small- and medium sized businesses to open accounts online.[22] Apps now have integrated check scanning to facilitate deposits and digital

22 DBS, n.d., It's simple to open your new account – anytime, anywhere, https://www.dbs.com.sg/personal/deposits/bank-with-ease/addon-casa and DBS, n.d., Business Digital Account https://www.dbs.com.sg/sme/day-to-day/accounts/digital-account.

signature features to facilitate transactions. Measures such as multiple-factor identification validation and the use of strong end-to-end encryption further improve security.

Figure 5: Observations on how cloud has enhanced FI resilience and supports economic recovery

Source: ACCA, 2021

Cloud underpins the use of new technologies for critical functions: back-office operations, compliance, KYC, AML, fraud detection

Cloud services allow FIs to use a wide range of technological innovations to derive value from data for their business. Cloud is playing an increasingly important role in an FI's ability to improve the efficiency of operations by facilitating the use artificial intelligence (AI) and big-data analytics. These new technologies can help reduce risks and improve resilience.

Furthermore, cloud supports the potential of greater operational efficiency by enabling the integration of business units through improved data sharing, the use of common data sets, more sophisticated data analytics and, ultimately, shared insights. This cloud-based functionality enables faster decision-making. Cloud-based business agility allows an FI to optimize operations and manage resources by leveraging tools such as AI (including image recognition and natural language processing), big data analytics and the Internet of Things (IoT). FIs can leverage these new tools and capabilities to increase revenue, cut costs, make business processes better and more efficient.

Cloud computing can help FIs more efficiently and precisely meet regulatory reporting requirements, such as the US Federal Reserve's Comprehensive Capital Analysis and Review.[23] Cloud-based AI and advanced analytics, using a range of FI datasets, can be used to improve an FI's intraday liquidity and risk calculations.

New regulations demand agility in compliance, and cloud technologies are helping FIs quantify credit risk, market risk and liquidity risk as rules evolve. Cloud technologies can improve the granularity and frequency of intraday liquidity and risk calculations, as well as using a wider range of scenarios with increasing volumes of data in a manner previously

23 US Federal Reserve System, n.d., Comprehensive Capital Analysis and Review. https://www.federalreserve.gov/supervisionreg/ccar.htm.

unavailable with legacy systems. This has proven to be important in the current economic situation, where a dynamic economic environment can lead to credit and counterparty risks that fluctuate beyond normal ranges. Improved capability to precisely analyze and forecast risk can enable better management of said risk.

As technology advances, so must the measures protecting customers, institutions and markets from sophisticated financial crimes. Cloud-based AI and advanced data analytics are being used to provide faster, more granular analysis of transaction surveillance data and data held across previously siloed operations of the FI (e.g., risk, finance, customer support, regulatory) to head off the risks to customers and the FI. These tools give FIs the ability to undertake more rapid and accurate know-your-customer analysis, anti-money laundering, identity theft and other fraud detection.

Risk-based approach to improve resilience, business continuity and disaster recovery

A risk-based approach[24] to security and data governance begins with identifying true risks and allocating resources based on a rational and proportionate analysis, prioritizing the mitigation of those risks. Risk-based strategies address all types of risks: cybersecurity, physical outages or disruptions, resilience, business continuity, data recovery and service provider concentration risk.

Risk-based strategies are essential to ensuring compliance, resilience, business continuity management (BCM) and disaster recovery (DR). The ability to replicate and operate data, applications and services across multiple data centers in disparate geographic locations is a standard approach to mitigating these risks.

Historically, FIs achieved these strategies by operating all data centers (operational, as well as redundant/back-up systems) to manage their workloads. The cost, relative to the expense of using cloud to achieve these strategies, was significant and, today, is still increasing. As FIs grew or merged (bringing together very different forms of IT infrastructure and data management), the cost and complexity of ensuring BCM and DR increased further.

Cloud provisioning reduces capital expenditures, mitigates the IT and data management challenges for merged FIs, and increases options for FIs to meet their security and data governance objectives. With cloud, FIs can operate “active-active” systems across multiple zones or regions, providing operational resiliency without the significant additional expenditure of a back-up. Should one active zone fail, the other zone is already active and can be automatically implemented at scale.

An FI can meet BCM/DR objectives by taking a few different approaches. Most multinational CSPs have data centers across the globe, boasting the highest quality security measures. With global resources available, an FI has many options to use cloud as a strategy to address redundancy and geographic diversity to enhance resilience with regard to cybersecurity, physical and environmental disruption and, if a concern, political risk.

- One approach, which would be the most conservative, is to maintain some on-premises infrastructure and replicate or complement the functionality of that infrastructure on a cloud platform, a.k.a. a ‘hybrid’ strategy.
- An FI can engage a single CSP and contract it to ensure reasonable geographic diversity between operational systems and redundant systems.

24 A risk-based approach can be summarized as a logical five step process, first determining your assets and who has control of the asset, identifying the threats and correspondingly, identifying vulnerabilities, assessing the likelihood of a threat will exploit a vulnerability, identifying and implementing the controls appropriate to mitigate the risks.

- A third option, if there is adequate interoperability between two CSPs: an FI can contract with multiple CSPs in a multi-cloud strategy.

As FIs transition to cloud services, cloud-based innovations can meet the needs of FIs and enhance their ability to fulfil the fundamental responsibilities of compliance, resilience and risk-management. Artificial intelligence and big data analytics are significantly improving FI security, fraud detection and capital reserve and risk analysis. Most multinational CSPs are perpetually looking and preparing for the newest threats, protecting their systems, networks and customers with the most up-to-date security controls.[25]

Many regulators are increasingly recognizing that CSPs utilize stringent standards to ensure they manage risks effectively. This is reflected in some of the most forward-leaning outsourcing guidelines that acknowledge the division of security responsibilities. Although ultimate responsibility for compliance remains with the FI, guidelines enable the shared-responsibility model for cloud; for example, where a CSP is providing Infrastructure as a Service (IaaS), the CSP is responsible for the security of its infrastructure and underlying services, while the FI is responsible for security of the data, applications and operations under their control.

New financial service products and services are built on the cloud

As demonstrated during the COVID-19 pandemic, new services from traditional FIs, merchants and e-commerce platforms, such as electronic payments and digital banking, have transformed the consumer experience. For example, in Singapore, the Association of Banks in Singapore (ABS) established PayNow, an electronic payments system that enables instant transfers among individual and merchant customers of major traditional banks in Singapore. Hong Kong's Faster Payment System (FPS) electronically links traditional banks with digital wallet systems such as Alipay, Wechat Pay HK and PayMe, enabling instant payments to merchants from traditional checking or savings accounts.

Beyond these newly digitalized, yet familiar experiences, traditional FIs and non-bank entities are offering new services such as mobile payments (e.g., Alipay, Apple Pay, Go Pay, Google Pay, Grab Pay and PayPal) and redefining the customer experience by integrating payment, real-time account management and trading functionality into mobile devices. These new digital-only services are based on cloud service platforms.

Digital or virtual banks (also called neobanks or "challenger banks") are on the rise in the region. Virtual banks are licensed but have no physical branches. Already accepted in the UK and Europe, where a number of virtual banks have established themselves with adequate capital and a growing customer base of digital-savvy individuals that do not feel the need for a bank to have a physical presence, Asia is seeing growth in the area.

Virtual banks often offer services at a lower cost to customers, such as lending to higher risk borrowers.[26] There is also a growing recognition among governments that virtual banks can act as a conduit to provide financial services to the previously unbanked and underbanked. With these bank accounts, citizens can establish credit-worthiness and participate more fully in the economy.

---

25 See Appendix I.
26 Fintech News, October 2019. What is Suptech? An Overview of this Rapidly Growing Space, https://fintechnews.ch/regtech/what-is-suptech-an-overview/31289/

- For example, Hong Kong is a leading market for virtual banks, having licensed eight since March 2019.[27] The Hong Kong government has promoted virtual banks as a way to reach underbanked small- and medium-sized businesses.[28] Some of the companies licensed are not traditional banks, including a retailer (Jardine, 7-11 franchisee for Hong Kong), a property developer (Hong Kong Land, the largest landlord in Central Hong Kong), a smart-phone maker (Xiaomi) and an online travel site (Ctrip), each with their own perspective on the needs and taste of consumers - bringing much needed innovation to the sector.
- Other governments are exploring licensing virtual banks, with Vietnam having licensed one to date (Timo) and Malaysia planning on licensing five virtual banks within the year.[29]
- With nearly 2.5 million citizens underbanked (40% of the population), Singapore has received 21 applications in a first round for virtual bank licenses, of which 14 met basic requirements.[30] Two entities are to be granted full licenses in 202 and three have been licensed for wholesale banking services.[31]

In addition to virtual banks, non-bank Fintechs have taken off in the region. From cryptocurrency services and ride-sharing payment systems to new platforms that bring customers to traditional FIs, new financial services—some niche, some broader—are being invented on cloud platforms, developed and commercially scaled. Several widely recognized startups are serving customers in ways that traditional FIs have been unable due to regulatory or business constraints. For example:

- Singapore based CodaPay processes payments from cardless customers across the region, enabling access to alternative payment channels for entertainment, telecommunications and e-commerce.[32] CodaPay is available in Indonesia, Malaysia, Singapore, Taiwan, Thailand and Vietnam.[33]
- In 2019, China's WeBank received a Hong Kong Monetary Authority (HKMA) virtual bank license to operate in Hong Kong. WeBank is the Tencent-backed digital bank start-up that offers retail banking to individuals and businesses in China.[34] Hong Kong based start-up WeLab has introduced WeLab Bank, virtual banking services and WeLend, an online lending platform, both operating in Hong Kong.
- In 2020, the Securities Commission Malaysia (SC) licensed CapitalBay, a fintech start-up that offers peer-to-peer (P2P) multi-bank supply chain financial services to small-and medium-sized businesses to help them with cashflow and lending needs.[35] CapitalBay uses cloud technologies to offer businesses and FIs a P2P platform that includes security features, propriety risk algorithms and credit assessment, among other big-data driven features, to enable streamlined supply chain financing with sustainable repayment terms that help SMEs better manage cashflow.[36]

---

27 KrAsia, 2019, Digital banks are coming to Southeast Asia, https://kr-asia.com/digital-banks-are-coming-to-southeast-asia
28 KrAsia, 2019, Digital banks are coming to Southeast Asia, https://kr-asia.com/digital-banks-are-coming-to-southeast-asia
29 FMT News, February 2020, Digital banking is changing Malaysia's financial landscape, https://www.freemalaysiatoday.com/category/leisure/2020/02/01/digital-banking-is-changing-malaysias-financial-landscape/
30 Crowdfund Insider, August 2020, Digital Banking: Singapore May be Ideal for Virtual Banks Offering Modern Financial Services as 40% of its Nearly 6 Million Residents are Underbanked, https://www.crowdfundinsider.com/2020/08/165949-digital-banking-singapore-may-be-ideal-for-virtual-banks-offering-modern-financial-services-as-40-of-its-nearly-6-million-residents-are-underbanked/.
31 Crowdfund Insider, August 2020, Digital Banking: Singapore May be Ideal for Virtual Banks Offering Modern Financial Services as 40% of its Nearly 6 Million Residents are Underbanked, https://www.crowdfundinsider.com/2020/08/165949-digital-banking-singapore-may-be-ideal-for-virtual-banks-offering-modern-financial-services-as-40-of-its-nearly-6-million-residents-are-underbanked/.
32 Crunchbase, n.d., Coda Payments, https://www.crunchbase.com/organization/coda-payments.
33 Tech Collective, August 2019, FinTech in Southeast Asia: new trends and market leaders, https://techcollectivesea.com/2019/08/30/fintech-in-southeast-asia-new-trends-and-market-leaders/.
34 Crowdfund Insider, 2019, Hong Kong Monetary Authority Approves Virtual Bank License for WeLab Digital Limited, https://www.crowdfundinsider.com/2019/04/146193-hong-kong-monetary-authority-approves-virtual-bank-license-for-welab-digital-limited/.
35 Tech Collective, August 2019, FinTech in Southeast Asia: new trends and market leaders, https://techcollectivesea.com/2019/08/30/fintech-in-southeast-asia-new-trends-and-market-leaders/. See also, https://www.digitalnewsasia.com/business/capitalbay-receives-sc-approval-operate-p2p-financing-platform.
36 Vulcan Post, RM2 Mil In Hand, https://vulcanpost.com/621713/startup-sme-cashflow-capitalbay-malaysia-funding/.

- PolicyPal, a digital insurance broker working with 30 global insurance companies began as an Android app and was the first business to complete its development time in Singapore's Fintech Regulatory Sandbox, before being licensed by the Monetary Authority of Singapore (MAS).[37] The company was recently acquired by Hong Kong's AMTD Group which, together with Xiaomi, owns AirStar Bank, one of the first eight virtual bank licensees in Hong Kong, as discussed above.[38] AMTD's Chairman and CEO, Calvin Choi, sees this as an opportunity to develop an innovative and comprehensive digital financial platform.[39]
- CreditVidya is a cloud native fintech headquartered in India whose underwriting technology is opening the loans market to over 250 million financially excluded citizens. Traditionally, financial institutions have been unwilling to lend to these citizens—typically with a daily household income of between $2 and $10—because they lack collateral and a credit history. Furthermore, processing the loans, which averages about $290 per applicant, has been too costly. CreditVidya's technology is reducing the cost of processing loans from about $2 to less than one cent, while overcoming a lack of credit history or collateral by leveraging loan applicants' digital footprints to measure their creditworthiness.
- Since 2008, both start-up and traditional investment advisors have developed roboadvisors: automated, algorithm-driven financial planning services with little to no human involvement. Roboadvisors are easy to set up and provide goal setting, portfolio management and other services, with low fees. Singapore-based StashAway received a capital markets license in 2017 from the Monetary Authority of Singapore (MAS).[40] In 2018, StashAway was licensed to offer services in Malaysia.[41] Singapore-founded Lumiq and Swiss-based Additiv also provide services in Singapore.[42] The Hong Kong-based 8 Securities launched a roboadvisory service called Chloe in Japan in 2015 and were followed there in 2016 by THEO, a Money Design company.[43]
- "Buy-now-pay-later" (BNPL) services are gaining popularity. These branded or white-label credit services enable consumers to take delivery of products from online and brick-and-mortar merchants. Australia's BNPL service, AfterPay, is exploring an acquisition of the Singapore-based EmpatKali BNPL service to expand in the Asia market. EmpatKali primarily focuses on the Indonesia market.[44] Other companies are also looking at bringing these services to Asia.

All of these services run on cloud platforms and would likely not have come to fruition without the affordability, capacity and scalability of cloud and the cloud ecosystem of services. From customer facing apps to big data analytics to back office functionality, cloud unleashes creative problem solving and provides the platform for innovation in financial services.

---

37 Fintech News, March 2020, HK-Based AMTD Acquires Insurtech Startup PolicyPal, https://fintechnews.sg/38448/insurtech/hk-based-amtd-acquires-insurtech-startup-policypal/.
38 Fintech News, March 2020, HK-Based AMTD Acquires Insurtech Startup PolicyPal, https://fintechnews.sg/38448/insurtech/hk-based-amtd-acquires-insurtech-startup-policypal/.
39 Fintech News, March 2020, HK-Based AMTD Acquires Insurtech Startup PolicyPal, https://fintechnews.sg/38448/insurtech/hk-based-amtd-acquires-insurtech-startup-policypal/.
40 StashAway, n.d., about StashAway, https://www.stashaway.sg/about.
41 StashAway, n.d., about StashAway, https://www.stashaway.sg/about.
42 Okhonko, Elena, 2018, Who is the Best Robo-Advisor in Asia, https://fintechnews.sg/20585/roboadvisor/best-robo-advisor-in-asia/.
43 The Asian Banker, 2017, Robo-Advisors Poised to Take Off, https://www.theasianbanker.com/updates-and-articles/robo-advisors-poised-to-take-off.
44 Electronic Payments International, 2020, Australia's BNPL services provider AfterPay eyes Asia expansion, https://www.electronicpaymentsinternational.com/news/australias-bnpl-services-provider-afterpay-eyes-asia-expansion/.

Growing importance of cloud to the role of financial services in the economic recovery, and continued economic growth after recovery

Many governments are establishing loan programs and grants to help workers and businesses weather the pandemic-driven economic crisis. Many of these programs call on FIs to forgive loans or manage government pay-outs to furloughed workers. Some require lenders to offer low- or no-interest loans to small businesses – processed much faster than the typical 60 days.[45] Some are better defined programs than others, but most require FIs to manage complex emergency programs with imprecisely defined eligibility requirements and benefit parameters.

Cloud computing is helping FIs scale up these specialized (and typically, online) services to meet customer needs in a time of crisis, while facilitating auditability and accountability. One feature of some lending programs is the ability of a small business to repay loans on a schedule in alignment with their varying cashflow.[46] Managing such irregular repayments without penalizing the borrower requires greater data management than what typical FI business processes and information technology are capable of. Therefore, cloud-based data analytics solutions are being deployed to meet the new demand while maintaining compliance with regulations.[47]

Although these programs vary from jurisdiction to jurisdiction, CSPs can work with FIs to offer solutions tailored to a particular program or CSP customer's needs. For the longer term, working with CSPs, FIs are able to envision new, rapidly deployed products and services that may serve well after the crisis passes.

Need for alignment of regulations across the region, in line with global standards

With the accelerated adoption of cloud computing, many regulators are moving quickly to encourage and oversee cloud adoption by implementing cloud guidelines and policies. The ACCA has observed a corresponding compliance challenge developing for FIs. As policies and guidelines are developed, several markets in the region have diverging regulatory requirements; published policies and guidelines on cloud have requirements with material differences.

Divergent policies add significant complexities for two reasons. Firstly, global FIs typically deploy globally standard systems and compliance is more efficient when there are fewer market-specific differences. Secondly, FIs typically outsource to CSPs that offer services across many markets and rely on global standards (e.g., SOC2, SSAE 18) for consistent rigorous review and reporting.[48] Therefore, the greater alignment among regulations across the region, the more efficient the compliance.

The impact of divergent compliance obligations is that in some markets, an FI would not be able to deliver the same innovative capabilities to their customers and/or costs of operations could significantly increase, even exceeding the point of viability. We are hopeful that as regulators adopt our recommendations, we will see greater alignment in compliance

45 Tech Radar, August 2020, How technology can support SME lending during the pandemic, https://www.techradar.com/news/how-technology-can-support-sme-lending-during-the-pandemic.
46 Tech Radar, August 2020, How technology can support SME lending during the pandemic, https://www.techradar.com/news/how-technology-can-support-sme-lending-during-the-pandemic.
47 Tech Radar, August 2020, How technology can support SME lending during the pandemic, https://www.techradar.com/news/how-technology-can-support-sme-lending-during-the-pandemic.
48 SOC2 is a reporting process based on a review of compliance with American Institute of Certified Public Accountants' (AICPA) Trust Services Principles (TSPs) to evaluate security, availability, processing integrity, confidentiality, and privacy. The Statement on Standards for Attestation Engagements No. 18 (SSAE 18) was created by the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) to reflect globally recognized international accounting standards. SSAE 18 aligns closely with the International Standard on Assurance Engagements 3402 (ISAE 3402).

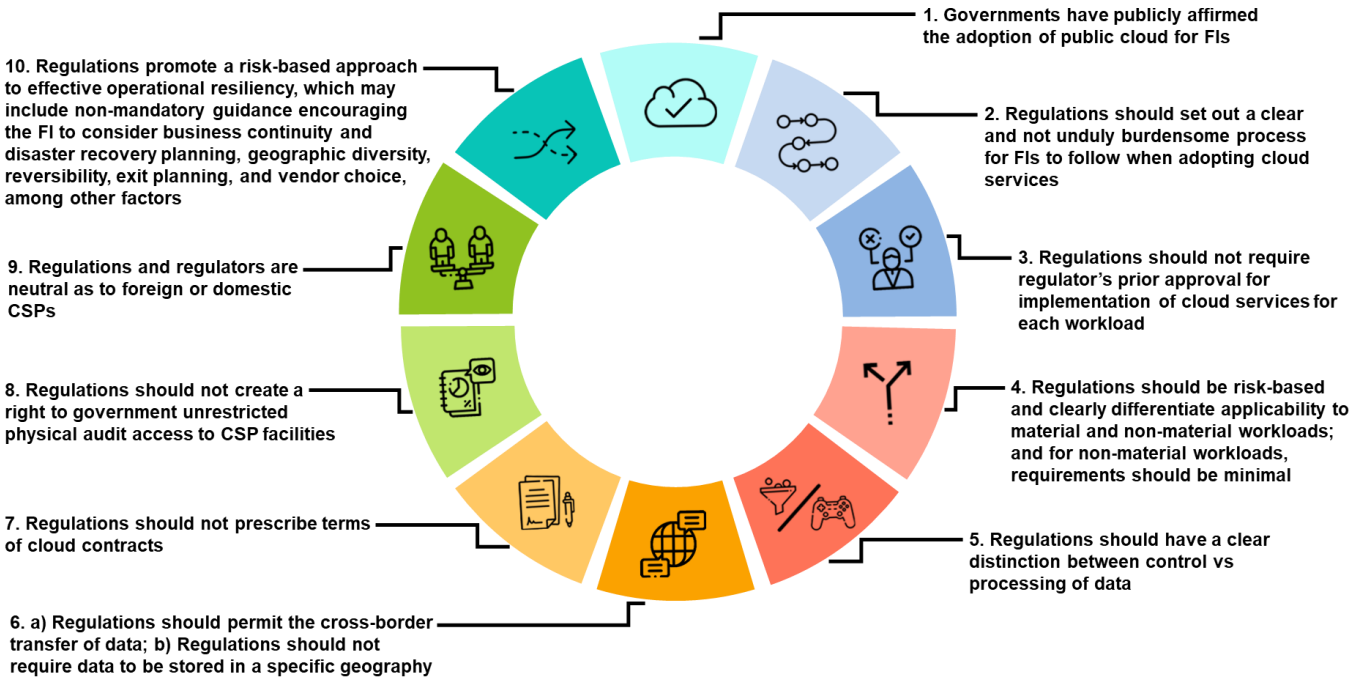
requirements across the region, and with global standards. ACCA encourages regulators across the region to align regulatory approaches. This includes taking a risk- and principles-based approach to regulatory requirements, and permitting the use of cloud for FSIs within a risk management framework. It also means enabling cross-border data flow, and permitting the processing of customer data appropriately protected on cloud, and without unduly burdensome regulatory processes.

Recommendations

The ACCA makes 10 recommendations – updated from our 2018 report – in order to capture a more nuanced understanding of FSI cloud by FIs and regulators. The objectives of the ACCA's recommendations are threefold:

- To help regulators understand how/why FIs use cloud services across many functions.
- To encourage regulators to align regulatory requirements and guidelines that impact cloud services within their jurisdictions and across different markets.
- To uphold the highest standards for compliance that will enable FI adoption of cloud using international standards and global best practices.

Figure 6: 10 Regulatory Recommendations



Source: ACCA, 2021

Understanding the revisions to recommendations

The ACCA's recommendations were revised to reflect the reality that FIs and regulators have been gaining a better understanding of what cloud computing is and how it fits into the FSI. In particular, we aim to highlight the ways that cloud fits within their compliance and oversight paradigm, and what adjustments to regulations and guidelines are in order.

Table 2: Summary table of recommendations and the justifications for scoring

Regulatory Recommendations	Justification for scoring direction
1. Governments have publicly affirmed the adoption of public cloud for FIs.	Public affirmation of public cloud adoption provides clarity that the regulator supports FI adoption of cloud services and acknowledges benefits.
2. Regulations should set out clear and not unduly burdensome processes for FIs to follow when adopting cloud services.	A clear regulatory process provides greater certainty and is therefore better for compliance and risk management. Opaque, uncertain and/or unduly burdensome processes tend to deter or impede adoption of new technologies.
3. Regulations should not require regulatory prior approval for implementation of cloud services for each workload.	Prior regulatory approval should not be required for an FIs adoption of cloud services for each workload or application moving to the cloud. Notification to the regulator where a material or critical workload is to be migrated to a cloud service should be adequate (but not require a "letter of non-objection" prior to migrating the workload to the cloud). Any notification processes should be clear and not overly burdensome or repetitive (e.g., a one-off outsourcing process should be sufficient for IAAS/PAAS type cloud adoption), and there should be a chance to "appeal" or consult with respect to any adverse decision by the regulator. Regulatory notification could be addressed in review of risk assessment frameworks.
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads and for non-material workloads requirements should be minimal.	Regulatory requirements should be proportionate to the risk associated with different workloads. This distinction is important, as it allows businesses to assess risk more clearly and align compliance and security with particular workloads. Criteria for assessing materiality should be defined clearly. If any, there should be minimal compliance requirements for non-material workloads.
5. Regulations should have a clear distinction between control vs processing of data.	This distinction is important, as it allows businesses to assess risk and assign controls and responsibility for compliance more clearly. Correspondingly, each party, the entity with control of the data and the entity processing data, will have very different roles vis-à-vis data management and protection, and therefore compliance.
6. Geographic Restrictions: a. Regulations should permit the cross-border transfer of data. b. Regulations should not require data to be stored in a specific geography.	Cross-border data flows should be allowed. This is consistent with the cross-border nature of financial services, as well as the nature of cloud-based data flows. Data localization requirements, or requirements for data to be stored in specific geographies, should be avoided, as this may create risk vulnerabilities for the FI and limit the efficiency of cloud deployment, which benefits from economies of scale. Such restrictions may also increase the cost of cloud adoption and restrict choice.
7. Regulations should not prescribe terms of cloud contracts.	Regulations may identify compliance objectives or principles, but should allow cloud contracts to be negotiated freely between CSP and FSI with maximum flexibility while meeting compliance obligations.
8. Regulations should not create a right to government for unrestricted physical audit access rights to CSP facilities.	Unlimited physical access to CSP facilities is not necessary for audits or oversight and creates security risks to the CSP and its customers. Alternatively, a certified audit conducted on a regular basis with reports made available to regulators can address oversight objectives.
9. Regulations and regulators are neutral as to foreign or domestic CSPs.	As a matter of best practice, we recommend that regulations should be neutral as to domestic and foreign CSPs. It is important to ensure an FI can select the most appropriate CSP to provide the best service, based on international standards and best practices, to meet their business objectives, as well as cost considerations.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.	To ensure greatest flexibility for FIs to manage resiliency, regulators should encourage a risk-based approach, which may include non-mandatory guidance encouraging the FI to consider factors such as business continuity and disaster recovery planning, geographic diversity, reversibility and exit planning, vendor choice, among other factors. Prescriptive regulations should be avoided.

Source: ACCA, 2021

Another update is the change from our scoring model, from a color-coded binary representation used in 2018, to an absolute numeric scoring. This will give regulators a more granular understanding of how they are doing on the journey toward greater cloud adoption in their market, and may be useful for market comparisons where regulators may see what areas can be improved, and what challenges they or their regulated community may face as FIs adopt cloud services in their market.

After a review of the banking sector's regulations, we offer the following analysis of 11 markets in the Asia Pacific. For reference, we evaluated the United Kingdom and the United States (both a federal regulator and one state regulator, as illustrative). The markets in the Asia Pacific are Australia, Hong Kong, Indonesia, India, Japan, Malaysia, the Philippines, Singapore, South Korea, Taiwan, and Thailand. For each market, we evaluated the banking regulations and guidelines against the recommendations to understand if the regulations or guidelines clearly comport to the recommendation. For each recommendation, we describe below the particular scoring criteria and explain in greater detail the focus of the recommendation.

Methodology: Recommendations Described, and Scoring Criteria

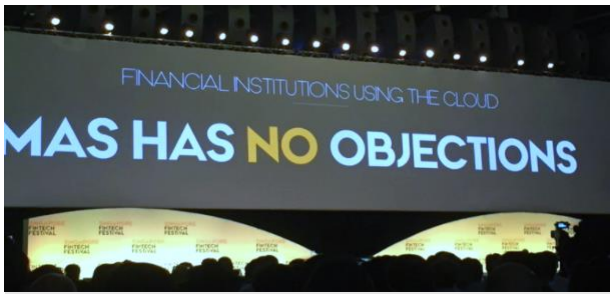
Recommendation 1: Governments have publicly affirmed the adoption of public cloud for FIs

Scoring

- 6 points: Yes, public cloud adoption is promoted in a public affirmation.
- 4 points: Benefits of public cloud have been acknowledged, but adoption not explicitly promoted.
- 2 points: Cloud benefits generally acknowledged, no mention of public cloud.
- 1 point: Implicit preference for private cloud or hybrid use of cloud OR no mention of financial sector using cloud.
- 0 points: Explicitly against public cloud.

In several markets, regulators have taken actions or made public statements which clearly affirm support for the use of cloud services by FIs. This may be in the context of government policy, regulations or guidelines, or a widely recognized public statement. Singapore stands out in this regard. In 2016, the Monetary Authority of Singapore (MAS) Managing Director, Ravi Menon, publicly declared during the Singapore Fintech Festival that MAS has no objections to financial institutions using cloud (see photograph).

Image 1: MAS announcement on cloud computing, 2016 Singapore Fintech Festival



Source: ACCA, 2016[49]

More recently, MAS is affirmatively promoting cloud. In August 2020, MAS announced that it will commit S$250 million over the next three years under the enhanced Financial Sector Technology and Innovation Scheme (FSTI 2.0), to support investment in early stage and large scale FinTech projects, including the use of cloud computing as one of five technologies that will "fundamentally transform financial services".[50] Governments that affirmatively express a positive view toward FI adoption of cloud provide an appropriate opening for an FI to begin discussions with the regulator on the adoption of cloud services by the FI. This is one of the clearest demonstrations of the changing views among regulators.

One particular area that is relevant to embracing cloud is how regulators view personal data that is encrypted. MAS accepted feedback during the consultation[51] in 2016 that the obligations which apply to "customer information" should not apply to information that is public, made anonymous or encrypted securely, and which cannot be used to readily identify the FSI's customers. The ACCA would recommend that all regulators consider taking the same approach to enable greater use of the cloud.

49 ACCA Twitter, 17 Nov 2016, https://twitter.com/accacloud/status/799102882955960320.
50 Yahoo Finance, August 2020, Innovation and technology adoption in financial sector accelerated, https://sg.finance.yahoo.com/news/innovation-technology-adoption-financial-sector-182849393.html.
51 Monetary Authority of Singapore, July 2016, Response to Feedback Received – Public Consultation on Guidelines on Outsourcing, https://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Response%20to%20Consult%20%20Outsourcing%20Guidelines%20Jul%202016.pdf.

Recommendation 2: Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services.

Scoring

- 6 points: Yes, regulations set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption (could be through a reference in the regulation itself or in accompanying cloud computing guidelines/ information papers). Such processes are proportionate, practical and not unduly burdensome.
- 4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.
- 0 points: No, there is no clear process or regulatory guidance on outsourcing or cloud adoption, and/or processes are unduly burdensome.

The ACCA strongly recommends that regulations should offer a clear process by which FIs can move to the cloud. A clear process provides greater certainty for compliance. Furthermore, the process should not be unduly burdensome.

In the first instance, we look for clarity on whether cloud computing use is explicitly indicated as a possible option for FIs. For example, does it appear as one of a number of services which fall under a FI outsourcing policy or guideline, or has the regulator developed a technology risk management framework that governs technology use by FIs?

In the United States, regulations of the Office of the Comptroller of the Currency, the primary federal banking regulator, set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption. The federal interagency body that establishes cross-agency principle-based policies, the Federal Financial Institutions Examination Council (FFIEC), has an Outsourcing Technology Services Booklet bringing together the range of applicable laws and regulations and detailing the procedure and requirements to follow when outsourcing technology, which the FFIEC has separately stated is applicable to cloud.[52] The several applicable regulations, along with a guidance booklet, provide clear compliance procedures to the FI adopting cloud services.

We are heartened to observe that most markets in this report have worked to clearly indicate the process by which cloud computing can be adopted by FIs, such as the HKMA's Supervisory Policy Manual (SA-2), which calls out "latest technology" in Section 1.1.3 enabling the adoption of cloud computing.[53] However, Malaysia BNM's Outsourcing Guidelines, which address "Outsourcing involving cloud services" in Section 11,[54] and Australia APRA's Information Paper on "Outsourcing Involving Cloud Computing Services" are more forthright in calling out cloud computing.[55]

Markets which score highest on this factor would have set out explicit processes by which FIs can adopt cloud. For example, many of the above-mentioned markets have regulations which detail due diligence and accountability mechanisms for FIs. At the same time, even if regulatory requirements and processes are clear, they should be proportionate to any risk and not be unduly burdensome. Unnecessarily burdensome and prescriptive requirements risk turning compliance into a "check-

52 FFIEC, n.d., Outsourcing Technology Services Booklet, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.
53 HKMA, n.d., SA-2 Outsourcing, http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf.
54 BNM, Oct 2019, https://www.bnm.gov.my/index.php?ch=57&pg=144&ac=849&bb=file.
55 APRA, 24 Sep 2018, Information Paper, Outsourcing Involving Cloud Computing Services, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf.

the-box" exercise and tend to place the responsibility of risk assessment on the regulator rather than the FI. This can deter or slow technology adoption and innovation.

Streamlined outsourcing arrangements/approvals for FIs

Regulatory requirements and processes should be streamlined as much as possible without compromising on security and compliance. The majority of cloud regulations today do not differentiate between cloud deployment models, i.e. the IaaS, PaaS, and SaaS delivery models. In addition, many regulations add unnecessarily onerous responsibilities for FIs when it comes to cloud adoption, by requiring outsourcing arrangements and approvals: FIs are generally required to execute outsourcing processes for each deployment of IT applications to the cloud, which can be highly repetitive, time-consuming, and inefficient. In addition, there is significant fragmentation among different regimes in APAC that require FIs to repeat such processes in every country (which is extremely burdensome for global or regional FIs that provide services cross-border).

For example, where FIs put their own applications on a third party CSP platform (e.g., outsourced IaaS or PaaS), retain full responsibility and control of such applications and data, and do not have operational access to it, we recommend that regulators only require FIs to secure a single FS regulator's approval or notification for such arrangement, to be executed only once for the overall platform development/cloud migration plan, and for all subsequent workloads and applications.

This approach will allow FIs to benefit from faster time to market and the ability to redeploy resources, from repetitive compliance management to higher-value add propositions.

Recommendation 3: Regulations should not require regulator's prior approval for implementation of cloud services for each workload.

Scoring

- 6 points: No regulator's approval necessary – (compliance with global standards and international third-party certifications are adequate).
- 4 points: Regulations do not require regulator's prior approval (formal or de facto) for non-material workloads.

  For material workloads, a regulator's approval (formal or de facto) is required, but it is not required for each workload.

  The approval process should be clearly described, follow a transparent and objective process with clear requirements, prompt deadlines and criteria for approval and offer the FI or CSP a right to appeal.

  There may be a requirement to 'inform' or give 'notice' to the regulator on occasions a material workload is moved to a CSP, but the notification process does not require an FI to wait for a letter of non-objection before proceeding with the move of the workload to a CSP.
- 2 points: Regulations require prior approval (or notice to the regulator and a letter of non-objection) for each CSP/Bank relationship and not each workload, but do not have the clarity of process described for 4 points. The approval process is not clearly described, or does not follow a transparent and objective process with clear requirements, prompt deadlines and criteria for approval and offer the FI or CSP a right to appeal.
- 0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.

In some markets, the regulator requires approval for each occasion an FI intends to place a workload on a cloud service. The process can be highly repetitive, lengthy and opaque, which can impede cloud deployment. In some markets, only notice is required, but FIs are required to await a 'notice of non-objection' or similar assent by the regulator before proceeding to transfer the workload to a CSP. This effectively constitutes a 'de facto' approval requirement.

For an outsourcing arrangement with a CSP, there should be no requirement for a regulator to approve the use of cloud services by an FI. Rather than requiring approvals or de facto approvals, regulators should consider the FI's risk-based analysis and how the standards, best practices and certifications of a CSP align with objectives. CSPs, particularly if they are multinational service providers, typically maintain their services to meet the highest international standards and global best practices to meet the demanding needs of global FIs. Furthermore, it is notable that FIs manage compliance through their risk-based policies with outsourcing vendors (including CSPs), and oversight should focus on an FI's compliance with the risk management expectations of the regulator.

One of the key benefits of cloud computing is the ability to move workloads efficiently and quickly as needed in an agile and scalable environment. Onerous approval processes (whether formal or de facto) can deter or delay technology adoption and innovation. A better alternative to approval for each workload would be to integrate the use of a risk assessment framework when the FI engages the CSP. In this scenario, rather than approval, there is a requirement to inform the regulator when an FI engages a CSP or moves a new workload to the CSP. Notification to inform provides the regulator the opportunity to consider compliance without delaying the deployment unnecessarily.

Any regulatory process should be proportionate to the risk involved. As for any approvals or notifications (if absolutely necessary), these should be limited to critical or at least material workloads. Furthermore, as noted above, all regulatory processes should be streamlined to the extent possible. For example, where FIs put their own applications on a third party outsourced platform (IaaS/PaaS), we recommend that regulatory outsourcing processes (or respective approvals/notifications) are not required from FIs

for each workload but, instead, should be executed only once for the overall platform development/cloud migration plan, and suffice for all the workloads and applications developed afterwards.[56]

56 This recommendation is also aligned with Principle 8 of Proposed ASIFMA's Principles for Public Cloud Regulation, issued in March 2021: "Regulators should also provide flexibility and allow such notifications to be made at a higher level, such as for an overall system platform development plan or a cloud migration plan; and in case any additional notifications are considered necessary throughout the plan, FIs and regulators can work together early to identify and focus their attention only on the critical components of the plan." https://www.asifma.org/wp-content/uploads/2021/03/final-proposed-asifma-principles-for-public-cloud-regulation-1.pdf.

Recommendation 4: Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal

Scoring

- 6 points: Yes, regulations clearly differentiate applicability to material and non-material workloads, and regulations for non-material workloads are light touch (minimal), if any. Criteria for assessing materiality are clearly defined.
- 4 points: Yes, to an extent. Regulations clearly differentiate applicability to material and non-material workloads, and non-material workloads are exempt from additional documentary requirements (applicable to material workloads), but other onerous regulatory requirements apply to non-material workloads.
- 2 points: Differentiation (materiality is defined) is made but same regulatory requirements apply to both material and non-material workloads.
- 0 points: No differentiation and all workloads are treated equally.

Regulations should be clear as to their applicability to material workloads or non-material workloads. This distinction corresponds to the risks to the FI. Risks to non-material workloads are much lower or often present no risk to the FI. Therefore, non-material workloads should not be subject to the same compliance burden as material workloads or any regulations that could bar the use of cloud computing, as risks are low and oversight requirements are nominal. Further, there should be recognition that not all material workloads are critical workloads; for critical workloads, there may be particular requirements.

If there are regulations applicable to non-material workloads, they should be minimal. Distinguishing regulations for material versus non-material workloads allows an FI to align security controls to actual risk, providing for more controls related to material workloads than for non-material workloads, and focusing resources on areas of higher risk.

An illustration of good policy is the Australian Prudential Regulation Authority's (APRA) Prudential Standard CPS 231 governing outsourcing. CPS 231 only applies to the outsourcing of material business activities. APRA defines a material business activity as one that, if disrupted, has the potential to significantly impact the FI's business operations or its ability to manage risks effectively. The internal audit and risk management functions are both considered to be material business activities.

Material outsourcing is also subject to prior consultation with APRA and a notification requirement once the entity has entered into the agreement. Non-material outsourcing arrangements are not subject to these requirements, however, they are subject to certain information security requirements, as per CPS 234 Information Security, such as the need to evaluate an outsourced provider's information security controls' design; ensuring that the provider's information security capability is commensurate with the potential consequences an information security incident will have on the information assets it manages; and that the nature and frequency of its systematic testing of security controls is at an effective level commensurate with factors such as the criticality and sensitivity of the information asset.

Similarly, in Taiwan, Article 19-2 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation clearly defines that material operations and different regulations apply with respect to material and non-material operations.[57] In Malaysia too, the Risk Management in Technology (RMiT) guidelines were updated in June 2020 and prior approval is only required for critical systems. In addition, clear distinctions have been made between critical and non-critical systems.[58]

57 Financial Supervisory Commission, 2019, Press release on Amendments to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=-201910220020&aplistdn=ou=news,ou=multisite,ou=english,ou=ap_root,o=fsc,c=tw&dtable=News.
58 BNM, June 2020, RMIT, https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078.

Recommendation 5: Regulations should have a clear distinction between control vs processing of data

Scoring

- 6 points: Yes, there is a clear distinction between an entity that is a controller versus one that is a processor of data.
- 4 points: Draft regulation makes distinction.
- 2 points: Unclear or ambiguous (e.g. mentions, but no definition).
- 0 points: No distinction.

A clear distinction between control and processing (and the entity responsible for each – the controller and the processor) is important, as it aids regulators' understanding of the different responsibilities between the entity that has control of data and the entity that processes the data, and ensures there is clarity as to which entity is in a position to affect compliance. In the context of data management for FIs, the data controller is the entity that makes decisions on how and why the data is being processed. The data processor is to be distinguished from the data controller, as they only process the data on behalf/at the behest of the data controller.

The distinction between controller and processor is important, because the responsibility for compliance for outsourced activities cannot be outsourced. For many cloud services (e.g., Infrastructure as a Service' (IaaS) and 'Platform as a Service' (PaaS)), the CSP is typically only a 'data processor' because it does not make decisions or have control over how or why data is being processed. In fact, it rarely has access to its customers' data. The FI typically is the 'data controller', because they make all decisions as to how and why data is being processed. An important aspect of this is how risk is allocated. Risk, and therefore liability, cannot be outsourced, and recognition of this fact must be clearly distinguished in regulations.

Most often, we find the distinction between controller and processor in personal data protection or privacy laws. However, in some markets the distinction is made in the context of FSI outsourcing guidelines or regulations. Many markets have bank secrecy laws which have not been updated to reflect how data and information are used today. We recommend that such laws be updated to take into account the use of cloud services (where obtaining individual consents from FI customers is not feasible for the FI or CSP).

Recommendation 6: Regulations should permit cross-border data transfers and should not require data to be stored in a specific geography

Scoring	
a. Regulations should permit the cross-border transfer of data.	• 3 points: Yes, cross-border transfers are allowed with appropriate safeguards. • 1 point: Not allowed, with some exceptions. • 0 points: Not allowed.
b. Regulations should not require data to be stored in a specific geography.	• 3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards. • 1 point: Only 'white listed' jurisdictions allowed. • 0 points: Data must be stored in specific geographic locations.

ACCA observes three types of geographic restrictions that are contrary to the successful, most efficient use of cloud computing:

- One where an FI within the jurisdiction, or with customers that are citizens/residents of a jurisdiction, is not allowed to transfer its data outside of that jurisdiction. This is called 'data localization'.
- Another is where an FI within a jurisdiction must maintain a copy of its data within the jurisdiction, even if the data is also transferred outside of the jurisdiction. This is another flavor of data localization.
- A third variation on data location restrictions may require data to be maintained in particular geographic locations for what is perceived by the regulator as greater resilience. For example, an FI in one city may be required to maintain redundancy in another city many miles away, but within the jurisdiction of the regulator.

Data localization reflects the incorrect perception that in order to have oversight and access to data, it must be stored within the jurisdiction of the regulator. However, this perception overlooks the reality that so long as the regulated FI is within the jurisdiction, the regulator has access to all that FI's data through its oversight capacity vis-à-vis the FI. This is consistent with existing practices where an FI is not using cloud services.

Geographic restrictions with the objective of greater resilience, which require data be maintained within the jurisdiction of the regulator, adds a justification premised on another misperception. Indeed, if an FI is located in one city and only maintains redundancy within that city, there is a risk if that city is subject to environmental risks that could disable both the operational data system and the redundant system. In this case, it makes sense to mandate that the redundant system be located in another city. But that city need not be within the regulator's jurisdiction.

In reality, the same safeguards of geographic distance and distinction can be met with data centers located outside the jurisdiction. As major CSPs operate data centers across the globe, their resources can serve an FI from several locations; indeed, in some cases, multiple locations provide much better redundancy with the highest security standards.

In the United States, the regulations of key federal regulator, the Office of the Comptroller of the Currency (OCC), do not restrict cross-border data transfer or require data localization. However, the federal interagency body that establishes cross-agency principle-based policies, the Federal Financial Institutions Examination Council (FFIEC), notes that regulated entities which use foreign-based third party service providers (or domestic service providers that subcontract to foreign-based firms) must comply with applicable US laws such as Section 501(b) of the Gramm-Leach-Bliley Act, which stipulates safeguards for customer data. [59] As US FI's are subject to state law, we also examined the New York law, as many multinational FIs are headquartered in New York, and the New York State Department of Financial Services (NYDFS) regulations also do not restrict cross-border data transfers or require data localization.[60]

59 FFIEC, n.d., Gramm-Leach-Bliley Bill, https://www.ffiec.gov/exam/infobase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf.
60 New York State, n.d., 23 NYCRR 500, https://www.dfs.ny.gov/industry_guidance/cyber_faqs.

Recommendation 7: Regulations should not prescribe terms of cloud contracts

Scoring

- 6 points: Regulations are not prescriptive as to terms of a cloud contract. Regulations may require that there should be a contract with the CSP and the contract must address regulatory requirements/compliance – without specificity (regulations do not specify any prescribed terms to be included in the cloud contract) OR regulations state there should be a contract with the CSP and within that contract, specific principles or concepts that should be addressed (e.g. security, limits on data use responsibility for subcontractors, data location, rights to audit, exit provisions) OR regulations do not specify whether there should be a contract with the CSP.
- 2 points: Regulations have overly detailed requirements for the cloud contract, but do not go to the extent of prescribing specific contractual language.
- 0 points: Regulations prescribe specific contractual terms/language OR set out a prescribed form of cloud contract.

We recommend that regulations may identify compliance objectives or principles, but should allow cloud contracts to be negotiated freely between CSPs and FIs with maximum flexibility to meet compliance obligations. The terms of a contract between an FI and CSP must align with the particular arrangement for services. A wide range of cloud services are available for contracting, and the terms of the contract must reflect the specifics of the particular engagement. A regulatory requirement for specific terms or provisions may not be fit for the purpose of the contract. It is more valuable that the compliance objectives or principles be described, so it is clear to the FI and CSP what topics must be covered in the contract to meet the regulator's expectations.

We have observed in some draft guidelines – possibly due to anachronistic regulations – that there are sample SLAs provided for use, which could be misconstrued by an FI as a de facto requirement. In other regulations, there may be specific contractual terms or clauses which the regulator requires the FI to include within their cloud contracts. We would recommend that these be removed from regulations to enable a broader range of approaches to meet compliance requirements.

In Hong Kong, the requirements laid out in SA-2 provide that the outsourcing agreement clearly indicate the outsource provider's contractual liability and obligations, and that it includes a clause allowing for supervisory inspection of the outsource provider's operations and controls that relate to the outsourced activity.[61] The other regulatory requirements are presented as objectives. There are no prescribed terms. In Japan, the FSA's Comprehensive Guidelines for Supervision of Major Banks describes the general topics for contracts. Contracts should include the contents and level of service to be provided, and the procedures for cancellation; responsibility of the outsourcing contractor when the service is not provided as specified under contract, as well responsibility of payment of damages that may arise with regard to the outsourcing, including the provision of collateral; contents of the reports that the bank would receive from the outsourcing contractor; and arrangements concerning how to meet requests from the financial authority in relation to inspection and supervision.[62]

61 HKMA, n.d., SA-2, Sections 2.5.1 and 2.8.2 https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf.
62 FSA, 2 Jul 2014, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf.

Recommendation 8: Regulations should not create a right to government unrestricted physical audit access to CSP facilities.

Scoring

- 6 points: There is no regulatory requirement of a right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports.
- 2 points: It is not clear if regulations require the CSP to provide the regulator with unrestricted physical access.
- 0 points: Regulations specify that unrestricted physical access is required.

It is important for a regulator to be able to audit the activities of an FI. However, when that activity involves a CSP's data centers, there is no need for the regulator to have direct – and absolutely unlimited – access rights to enter the CSP's facilities at will. Where an audit involves an FI, the FI can provide – on their own premises – access to all data, applications and processes undertaken using the CSP's services.

Recognizing the unique circumstance for regulated entities, CSPs generally provide audit and inspection rights to regulators through the regulated entity, who is the CSP customer. Regulators generally find inspection of the CSPs controls through third-party or FI audit reports and discussions with the CSP to be sufficient. In some cases, a regulator may expect a right to audit a CSP's facilities with reasonable notice and within a reasonable scope of access – with the participation of a representative of the FI. It is important that the CSP be allowed reasonable control over access to their facilities for the security of other customers. In addition, it is not feasible for CSPs to accommodate data center visits by every regulator on behalf of each FI customer (even once a year, much less more frequently), as well as accommodating such requests by FIs themselves.

In the UK, there is no regulatory requirement for unrestricted physical access for audit. In fact, it is clear that regulators and FIs can rely on third-party audit reports for compliance. FG 16/5 provides instructions on a limited approach towards physical audit and access rights to FSI data under access to business premises.[63]

63 FCA, July 2016, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf.

Recommendation 9: Regulations and regulators are neutral as to foreign or domestic CSPs

Scoring

- 6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.
- 2 points: Some clear distinction in regulations for domestic CSPs disadvantaging foreign CSPs (e.g. requires local address, local representative office).
- 0 points: Companies need to be locally registered or there is a clear preference for cloud contracts to be given to local companies.

As a matter of best practice, we recommend that regulations are neutral, as between domestic and foreign CSPs. Regulations that disadvantage foreign CSPs vis-à-vis domestic CSPs may restrict choice and price competition, and thereby hinder technological advancement.

Generally speaking, multinational service providers are well positioned to leverage the economies of scale and global best practices to offer the resources and the expertise to maintain the highest standards of compliance, reliability and cybersecurity. These multinational service providers may, as a result, have capacities well beyond smaller providers and, in many cases, have much more experience in addressing cybersecurity proactively and preventatively. Governments often rely on private sector multinational CSPs for their forensics capabilities in understanding cyber threats and responding to incidents.

Further, these companies typically implement the highest levels of international standards and best practices to ensure their customer's data safety and compliance with legal and regulatory obligations. Large-scale multinational CSPs can often offer greater operational consistency, which is important to multinational FIs, including local FIs looking to expand beyond national borders. In addition, the scale of the services offered by multinational providers often allows them to offer cloud services at a lower cost and deliver operational consistency across regions, facilities and service offerings.

Recommendation 10: Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.

Scoring

- 6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.
- 4 points: Regulations promote a risk-based approach to operational resiliency and are not prescriptive, but do not include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.
- 0 points: Regulations related to operational resiliency do not focus on a risk-based approach to resilience or are prescriptive.

Regulators should encourage a risk-based approach to address resilience with a recognition that cloud computing can enhance resiliency. To ensure the greatest flexibility for an FI, regulators should include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors to address risk.

Regulators should encourage FIs to consider their existing infrastructure risk profile against the risk profile when using cloud services. For example, some FIs may operate one or several data centers in a city; the deploying of cloud services in the same metro area presents similar risks. If the FI can deploy across several geographical location, the operational resilience for the FI has increased due to geographic diversity, with regard to cloud services.

Regulators should encourage an FI to consider the benefits of cloud computing as part of risk-based contingency plans for emergencies and disasters, recognizing that the adoption of cloud supports or improves the ability of an FI to remain in operation in the case of an interruption. Regulators should provide guidelines (including recovery target objectives) with regards to how a CSP and FI can work together to reduce the time of disruption in case of emergencies or disasters.

Although ACCA makes no recommendations regarding the strategies by which an FI may address risk, regulators may want to understand how some FIs are looking at interoperability and data portability in the context of resilience, BCM and DRM. Some FIs want to use the services of one CSP while retaining reversibility or active-active redundancy – the ability to replace the services of the primary service provider with that of on-premises facilities – or, with active-active, simultaneously or for redundancy use the services of another CSP. Interoperability also allows an FI to use multiple CSPs to meet their specific needs. For example, multi-cloud strategies, which involves outsourcing to more than one CSP (each with their own risk profile), enables an FI to select a CSP based on value for money, distinct services offered, or to address vendor diversity.

Currently, CSPs have customizable services which allow each to offer unique services. A risk-based approach integrating interoperability and reversibility for data management allows FIs to select their preferred service from different CSPs, allowing FIs to achieve greater flexibility in their operations. Again, for each such decision, the FI must consider the risk profile for implementation.

A recent topic of concern among regulators and FIs is systemic or concentration risk, the risk associated with a critical mass of FIs relying on a single vendor (CSP or otherwise). It is worth noting that most regulators recognize that systemic or concentration risk across the sector can only be addressed by regulators, not individual FIs. Individual FIs can take measures to manage

only their own risk, e.g., with respect to operational resiliency and avoiding vendor lock-in, by carefully selecting their CSPs and considering factors such as geographic diversity, reversibility, exit planning, and vendor choice. It would be beneficial for regulators to work together across the region to provide a clear and consistent definition of concentration risk, including how they want to record it.

Regulators should also recognize the technology risks in the existing stack and consider whether moving to the cloud improves the overall risk profile. A clear and consistent definition would in turn allow for FIs and their providers to develop appropriate solutions to mitigate the risk.

Market Scores and Ranking

From our analysis, the leading markets have fully achieved most, if not all, of our recommendations. FI regulators in Australia, Hong Kong, Philippines, Singapore, and Japan have made strong positive statements or, through their guidance, clearly support the adoption of cloud computing by the FSI. The laws of Japan and Singapore allow transfer of data outside the jurisdiction; their regulations do not require the regulator to approve an FI's move to the cloud, while regulators in these markets encourage interoperability (and in some cases, encourage FIs to consider data centers in geographically diverse locations, interoperability or multi-cloud solutions).

Beyond the leading regulators, there is a group of markets where the shift to cloud is more challenging, as some regulatory requirements may tend to impede cloud adoption and technological innovation in the FSI. There are variations on why this is the case for each of these markets (as reflected below in Table 1, Market Scores and Rankings). However, the two most notable examples of these markets are Thailand and India. India is challenging for several reasons, including a number of geographic restrictions and a requirement for approval for each workload an FI moves to the cloud.

Finally, there are four notable markets in which leveraging global CSP services for the FSI is currently very difficult: Indonesia, Malaysia, South Korea and Taiwan. The most challenging aspect of doing business in Indonesia is that regulations apply to all FI workloads, material and non-material, and for each time an FI moves a workload to the cloud, approval is required. Although Malaysia had the same requirements prior to 2019, recent reforms require approval for only material workloads, which is a notable improvement. South Korea's regulations restrict cross-border data transfer and may not be neutral as between foreign and domestic service providers.

Financial Services in Asia Pacific 2021: Market Scores and Ranking

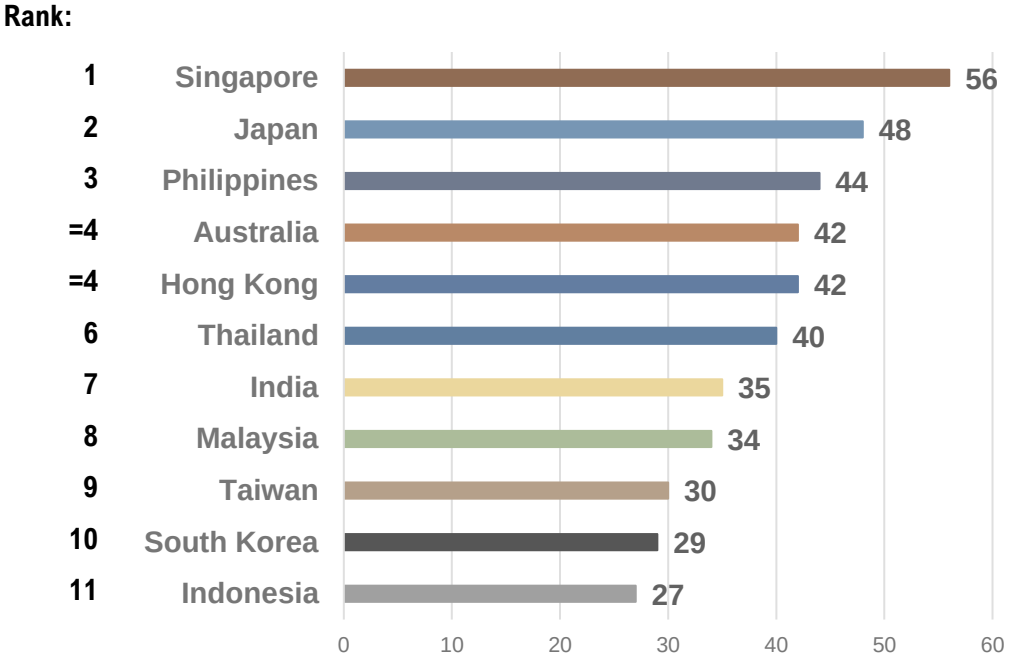
Table 3: Financial Services in Asia Pacific 2021: Market Scores and Ranking

REGULATORY RECOMMENDATION / MARKET & RANK	SG 1	JP 2	PH 3	AU =4	HK =4	TH 6	IN 7	MY 8	TW 9	KR 10	ID 11	UK -
1. Governments have publicly affirmed the adoption of public cloud for FIs.	6	6	6	4	2	2	4	6	2	2	6	6
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services.	6	6	4	6	4	4	4	4	4	4	4	6
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload.	6	6	0	0	0	0	4	0	2	4	0	6
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal.	6	0	2	6	2	4	2	4	6	4	0	6
5. Regulations should have a clear distinction between control vs processing of data.	2	2	2	0	6	6	4	6	0	6	4	6
6. Geographic Restrictions:												
6a. Regulations should permit the cross-border transfer of data.	3	3	3	3	3	3	1	3	1	1	1	3
6b. Regulations should not require data to be stored in a specific geography.	3	1	3	3	1	3	0	3	1	0	0	3
7. Regulations should not prescribe terms of cloud contracts.	6	6	6	6	6	6	2	2	2	2	2	6
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities.	6	6	6	2	6	6	2	0	6	0	0	6
9. Regulations and regulators are neutral as to foreign or domestic CSPs.	6	6	6	6	6	2	6	6	2	2	6	6
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.	6	6	6	6	6	4	6	0	4	4	4	6
TOTAL SCORE	**56**	**48**	**44**	**42**	**42**	**40**	**35**	**34**	**30**	**29**	**27**	**60**
MARKET	**SG**	**JP**	**PH**	**AU**	**HK**	**TH**	**IN**	**MY**	**TW**	**KR**	**ID**	**UK**

Source: ACCA, 2021

The overall scores and resulting market rankings are also represented in a bar chart below.

Figure 7: FSI Market Scores and Ranking (Bar Chart)



Source: ACCA, 2021

FSI ranking vs. general cloud readiness

In Figure 8, we provide a ranking of markets in this report and, for a point of reference, include on the Y-axis the ranking according to the ACCA 2020 Cloud Readiness Index, to give a sense of how well the financial services regulator is moving the industry toward cloud adoption as compared to the more general public policy objectives of their government (e.g. a Cloud-first policy for the public sector, encouraging broadband deployment and other factors).[64]

For the most part, rankings for the FSI correspond to the general cloud readiness of each market. The two outstanding markets are the Philippines and Korea, but for different reasons. The Philippines ranks low in general cloud readiness, yet is a strong performer as a FSI regulatory environment, conducive for FIs to move onto the cloud. However, Korea stands out for its overall cloud readiness yet poor scoring for the FSI. Data localization restrictions and detailed reporting requirements may prove to be restrictive. In addition, a recent revision of the Act on Promotion of Information and Communications Network Utilization and Protection now requires global ICT firms with more than 1 million daily users to designate a 'local agent' who can be held responsible in case of data breaches. These measures may cumulatively serve to slow the availability of cloud services to FIs.

64 Asia Cloud Computing Association, 2020, Cloud Readiness Index 2020, https://asiacloudcomputing.org/research/cri2020/

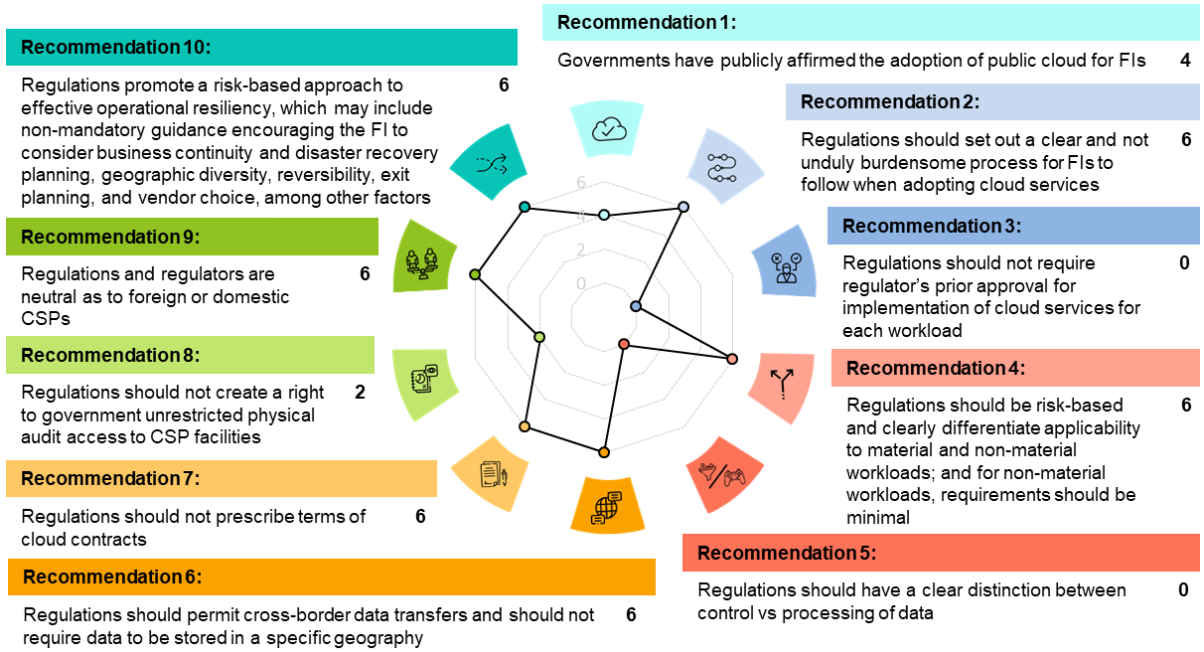
Figure 8: Market Rankings

Source: ACCA, 2021

Market Profiles

Australia

Figure 9: Australia's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 42

Market overview and key updates

A key update for Australia, since our 2018 report, is the updating of APRA's 2015 Information Paper on Outsourcing Involving Cloud Computing Services to address the increased interest in using cloud for higher-risk activities – such as critical systems – among Australian FIs.

Published in September 2018, the updated information paper seeks to ensure that FIs understand the risks involved in such arrangements and have adequate controls to manage them well. It also introduced a three-layer classification of risks (low, heightened and extreme) specific to the use of cloud computing services. Furthermore, the paper outlined the expectation for FIs to consult with APRA for arrangements involving heightened and extreme risk.

The 2018 Information Paper is significant, as it marked a "more open stance on cloud usage" by the regulator, and a departure from its historically reserved and skeptical view of cloud,[65] where APRA's 2015 position had "expressed reservations about the use the cloud for initiatives with heightened or extreme inherent risk",[66] and was expressly against the use of cloud for core systems.[67]

As it positively notes in its 2018 Information Paper, APRA's revised stance and increased confidence in the cloud can be attributed to progress in CSPs' strengthening of control environments, increased transparency of control environments and improvements to customers' ability to monitor their environment.

65 APRA, 2018, Cloud control: APRA evolves its stance on shared computing services, https://www.apra.gov.au/cloud-control-apra-evolves-its-stance-on-shared-computing-services.
66 ComputerWorld, 24 September 2018, Banking regulator warms to cloud computing, https://www.computerworld.com/article/3465025/banking-regulator-warms-to-cloud-computing.html.
67 Itnews, 6 July 2015, APRA updates cloud guidance for banks, https://www.itnews.com.au/news/apra-updates-cloud-guidance-for-banks-406164.

The 2018 Information Paper also reflects APRA's consultative approach in understanding and addressing risks, which has been fundamental in building trust and confidence and accelerating cloud adoption across Australian FIs.

For example, the National Australia Bank (NAB) noted that demonstrating through a framework that the migration of workloads to the cloud complied with security controls and internal standards allowed it to satisfy APRA that moving data to the cloud would be secure. This established a level of comfort with APRA for it to run cloud-based workloads at scale, allowing NAB to increase its speed of migration by bulk loading and bulk submitting workloads to APRA.[68]

Since it first began its cloud journey in 2017, NAB has migrated 800 applications to the cloud, and plans to host more than 80% of its systems on the cloud by 2023.[69] Digital bank Up Bank, the first retail bank in Australia to be hosted on the cloud, also worked closely with APRA and Google for a year prior to its launch in October 2019, allowing it to demonstrate to the regulator how the cloud led to improved security audits and disaster planning.[70]

In addition to the 2018 Information Paper, other notable regulatory developments that impact on cloud outsourcing are:

- On 1 July 2019, a new mandatory regulation, CPS 234 on Information Security, came into force. CPS 234 is APRA's first dedicated prudential standard for cybersecurity. As a legally-binding standard, the objective of CPS 234 was to boost the cyber-resilience of FIs and other APRA-regulated entities; it introduced new obligations, such as a mandatory breach notification requirement for material incidents to be reported to APRA within 72 hours. The related implementation guide, CPG 234 Information Security, was subsequently released to provide guidance on its implementation. It is worth noting that while the requirements in CPS 231 on Outsourcing apply only to the material outsourcing arrangements, CPS 234 imposes certain information security-related regulatory obligations that extend to non-material outsourcing arrangements.
- Australia's Consumer Data Right (CDR) Rules took effect on 6 February 2020, requiring Australia's four major FIs to share product reference data in a standardized format. The obligation to share consumer data relating to credit and debit cards, deposit accounts and transactions accounts, as per user request, began on 1 July 2020. CDR has been an accelerator for cloud adoption, as compliance has forced traditional FIs to revamp their legacy systems. Subsequently, many have taken the opportunity to move to the cloud and adopt other advanced technologies in the process.
- APRA's recent announcement of its Cyber Security Strategy for 2020 to 2024 has raised some concerns for ACCA members. Specifically, the note "Most notably, the new strategy aims to extend APRA's reach beyond our regulated entities to influence the broader eco-system of suppliers and providers they rely upon."[71] The remarks suggest that APRA may publish regulations that would directly impact CSPs.

68 Itnews, 6 November 2019, NAB reveals how it secured APRA's cloud blessing, https://www.itnews.com.au/news/nab-reveals-how-it-secured-apras-cloud-blessing-533238
69 Fintech Futures, 15 July 2020, NAB signs multi-year cloud deal with Microsoft, https://www.fintechfutures.com/2020/07/nab-signs-multi-year-cloud-deal-with-microsoft/
70 The Australian Financial Review, 19 November 2019, How banks and tech giants have convinced APRA to bless the cloud, https://www.afr.com/technology/how-banks-and-tech-giants-have-convinced-apra-to-bless-the-cloud-20191115-p53b2o
71 Australian Prudential Regulation Authority, 26 Nov 2020, Executive Board Member Geoff Summerhayes speech to Financial Services Assurance Forum, https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

Relevant regulator(s)

- Australian Prudential Regulation Authority (APRA)[72]
- Office of the Australian Information Commissioner (OAIC)[73]

Relevant regulation(s)

- CPS 231 Outsourcing (Prudential Standard)[74]
- CPG 231 Outsourcing (Prudential Practice Guide)[75]
- CPS 232 Business Continuity Management[76]
- CPG 233 Pandemic Planning (Prudential Practice Guide)[77]
- CPS 234 Information Security[78] and CPG 234 Information Security (Prudential Practice Guide)[79]
- CPG 235 Managing Data Risk[80]
- Information Paper on Outsourcing Involving Cloud Computing Services[81]
- The Privacy Act 1988[82]
- Competition and Consumer (Consumer Data Right) Rules 2020[83]

Summary of market alignment with the recommendations

Regulatory Recommendations	Australia's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**4 points: Benefits of public cloud acknowledged, but not explicitly promoted** The APRA Information Paper on Outsourcing Involving Cloud Computing Services acknowledges that "cloud computing services may bring benefits, such as economies of scale",[84] noting that 'cloud computing services' in the Information Paper refers to public, virtual private and community cloud arrangements, but excludes private cloud.
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**6 points: Yes, regulations set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption. Such processes are proportionate, practical and not unduly burdensome.** APRA sets out a clear process for FIs' cloud adoption through its *Information Paper on Outsourcing Involving Cloud Computing Services*.[85] The Information Paper guides FIs through the key considerations FIs should recognise at each stage of cloud adoption, such as when assessing materiality of the arrangement, selecting the solution, transitioning, as well as the notification and consultation process required for different types of material outsourcing arrangements. * FIs are required to notify APRA within 20 business days of executing a material outsourcing agreement. As part of the notification, FIs must provide a summary of the key risks involved in the outsourcing arrangement and the risk mitigation strategies it has in place to address these risks.[86]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.** Instead of requiring FIs to seek prior approval formally, APRA is informed of changes to an FI's risk profiles through a consultation and notification processes, giving APRA the opportunity to review and provide a notification of non-objection or objection. Since the implication of this process is that an FI has to wait for notice of non-objection before proceeding with the outsourcing, this consultation process is considered to be a 'de facto' approval process. APRA encourages prior consultation in instances where FIs' use of cloud computing services involves heightened or extreme inherent risks. While arrangements with heightened risks require formal consultation (that is meant to ensure FIs understand and have the capability to manage these risks) only after the FI has completed its internal governance process does APRA require that early engagement is sought for initiatives with extreme inherent risks, which gives APRA the opportunity to provide feedback and address any areas of concern before the FI commits resources to the initiative. Consultation is also required for material

72 APRA, https://www.apra.gov.au/
73 OAIC, https://www.oaic.gov.au/
74 APRA, CPS 231 Outsourcing (Prudential Standard), https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
75 APRA, CPG 231 Outsourcing (Prudential Practice Guide), https://www.apra.gov.au/sites/default/files/PPG-231-Outsourcing-Oct-06.pdf
76 APRA, CPS 232 Business Continuity Management, https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-232-Business-Continuity-Management-%28July-2017%29.pdf
77 APRA, CPG 233 Pandemic Planning (Prudential Practice Guide), https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-233-Pandemic-Planning-May-2013_1.pdf
78 APRA, CPS 234 Information Security and CPG 234 Information Security (Prudential Practice Guide), https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
79 APRA, CPG 234 Information Security (Prudential Practice Guide), https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf
80 APRA, CPG 235 Managing Data Risk, https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_1.pdf
81 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf
82 OAIC, The Privacy Act 1988, https://www.oaic.gov.au/privacy/the-privacy-act/#:~:text=The%20Privacy%20Act%201988%20(Privacy.other%20organisations%2C%20handle%20personal%20information.
83 Competition and Consumer (Consumer Data Right) Rules 2020, https://www.legislation.gov.au/Details/F2020L00094
84 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, Chapter 1, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf
85 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf
86 APRA, CPS 231, Paragraphs 37 and 38, https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf

Regulatory Recommendations	Australia's Scores and Justifications
	arrangements of all risk levels that involve offshoring. Moreover, all material outsourcing arrangements are subject to notification post contract-signing.[87]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**6 points: Yes, regulations clearly differentiate applicability to material and non-material workloads, and regulations for non-material workloads are light touch (minimal), if any. Criteria for assessing materiality are clearly defined.** APRA explicitly states that CPS 231 Outsourcing only applies to the outsourcing of material business activities. The outsourcing of material workloads are also subject to prior consultation[88] with APRA and a notification requirement once the entity has entered into the agreement, whereas non-material outsourcing is not. APRA defines a material business activity as one that, if disrupted, has the potential to significantly impact the FI's business operations or its ability to manage risks effectively. The internal audit and the risk management functions are both considered to be material business activities. Non-material outsourcing arrangements are, however, subject to certain information security requirements as per CPS 234 Information Security, such as the need to evaluate an outsourced provider's information security controls' design; ensure that the provider's information security capability is commensurate with the potential consequences an information security incident will have on the information assets it manages; and that the nature and frequency of its systematic testing of security controls is at an effective level commensurate with factors such as the criticality and sensitivity of the information asset etc.[89]
5. Regulations should have a clear distinction between control vs processing of data	**0 points: No distinction.** Australia's Privacy Act does not distinguish between data processors and controllers.
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, present, with appropriate safeguards.** Cross-border transfer of data is permitted. However, FIs are required to consult with APRA before entering into a material outsourcing agreement that involves cross-border data transfer.[90]
b. Regulations should not require data to be stored in a specific geography	**3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** There are no specifications of geographies for data storage. However, the Information Paper encourages FIs to consider Australian-hosted cloud options to eliminate additional risks.
7. Regulations should not prescribe terms of cloud contracts	**6 points: Yes, regulations are not prescriptive as to terms of a cloud contract. Regulations may require that there should be a contract with the CSP and the contract must address regulatory requirements/compliance -- without specificity (regulations do not specify any principles or prescribed terms to be included in the cloud contract) OR regulations state there should be a contract with the CSP and within that contract, specific principles or concepts that should be addressed (e.g. security, limits on data use responsibility for subcontractors, data location, rights to audit, exit provisions) OR regulations do not specify whether there should be a contract with the CSP.** CPS 231 lists 16 baseline matters that must be included in the cloud contract.[91] In addition, all outsourcing arrangements must be contained in a documented legally binding agreement, except where otherwise provided in CPS 231.[92] The Information Paper on Outsourcing Involving Cloud Computing Services stresses the need for cloud contracts to include an APRA-access clause.[93]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**2 points: It is not clear if regulations require the CSP to provide the regulator with unrestricted physical access.** According to CPS 231, although APRA will seek to obtain the information it requires from the FI, it still requires that outsourcing agreements include the right for it to conduct on-site visits to the service provider that it may undertake if deemed necessary. APRA qualifies that it will 'normally' inform FIs of its intention to undertake an on-site visit to a service provider.[94] The Information Paper on Outsourcing Involving Cloud Computing Services reiterates the need for FIs to include an APRA-access clause in the cloud contract that would give APRA this access right.[95]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** There is no distinction drawn in outsourcing regulations, nor preference for domestic CSPs, provided by regulators.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance	**6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** APRA recognizes that the risks associated with the use of cloud computing services will depend

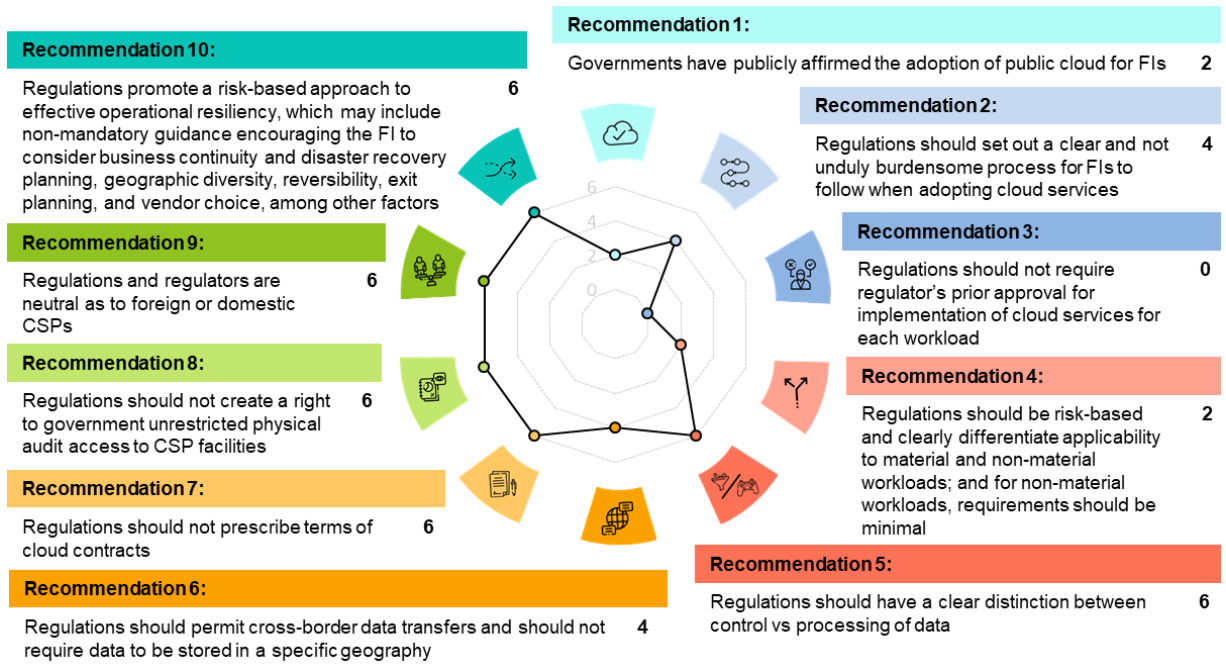
87 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf
88 While CPS 231 only specifies consulting as a requirement for offshore outsourcing, the subsequent information paper on outsourcing involving cloud services states that consultation, after internal governance processes are completed, is required for 'Heightened' material outsourcing arrangements, and encourages early consultation with the regulator for 'Extreme' material outsourcing arrangements. Based on the information paper, the only type of material outsourcing exempt from the consultation requirement are low-risk arrangements that do not involve offshoring.
89 APRA, CPS 234, Paragraphs 16, 22, 28 and 34, https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
90 APRA, CPS 231, Paragraph 39, https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
91 APRA, CPS 231, Paragraph 29, https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
92 APRA, CPS 231, Paragraph 23, https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
93 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, Page 13, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf
94 APRA, CPS 231, Paragraph 34, https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
95 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, Page 13, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf

Regulatory Recommendations	Australia's Scores and Justifications
encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	on the nature of its usage and expects all risks to be managed appropriately, commensurate with their inherent risk. As per the Information Paper on Outsourcing Involving Cloud Computing Services, APRA-regulated entities must develop contingency plans that allow for the cloud computing service to be provided through alternate means (e.g. transitioned to an alternative service provider or brought in-house), if required. APRA notes that this would typically be achieved through: 1) the development and periodic validation of exit strategies, including consideration of the contractual and technical ability to isolate and clearly identify IT assets for transition to another arrangement or in-house; and 2) consideration of the removal of sensitive IT assets from the provider's environment (including from backups and other copies).[96]

96 APRA, Information Paper on Outsourcing Involving Cloud Computing Services, Page 13, https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services_0.pdf

Hong Kong

Figure 10: Hong Kong's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 42

Market overview and key updates

Hong Kong FIs have benefited from the Hong Kong Monitory Authority's (HKMA) technology-neutral outsourcing and technology risk management (TRM) regulations, which have facilitated the uptake of cloud and cloud-based technologies. This has allowed HKMA's regulatory frameworks to remain mostly unchanged since the last publication of this report.

The HKMA has also embarked on a range of initiatives to nurture technological innovation by FIs, including the authorization of virtual banks. Hong Kong is a leading market for virtual banks, having licensed eight since March 2019.[97] Having recognized the benefits to competition and consumer choice that would come with the introduction of branchless, virtual banks, HKMA's guidelines for virtual banks allows non-banking companies to be eligible for virtual bank licenses, stirring competition in the traditional banking sector and creating an impetus for greater technological innovation in the sector.[98]

That said, it is worth recognizing that while the HKMA oversees the banking sector, insurance companies and securities and futures markets are regulated separately by the Insurance Authority (IA) and Securities and Futures Commission (SFC), respectively. As such, conditions for outsourcing to the cloud differ significantly even within the financial services industry.

While this report focuses on banking regulations, it is worth noting some of the more restrictive approaches taken by the SFC, for example through data localization requirements introduced through an October 2019

97 KrASIA, 21 August 2019, Digital banks are coming to Southeast Asia, https://kr-asia.com/digital-banks-are-coming-to-southeast-asia
98 Fintech Magazine, 15 September 2020, Hong Kong's digital banking begins with eight virtual banks, https://www.fintechmagazine.com/banks-and-challenger-banks/hong-kongs-digital-banking-begins-eight-virtual-banks

circular on the use of external electronic data storage,[99] which may weigh on FinTech innovation. These actions are notable in that they may allow other regulators in the region to consider more stringent restrictions that are contrary to our recommendation.

Relevant regulator(s)

- Hong Kong Monetary Authority (HKMA)[100]
- Privacy Commissioner for Personal Data (PCPD)[101]

Relevant regulation(s)

- Guideline on Authorization of Virtual Banks[102]
- SA-2 "Outsourcing"[103]
- TM-G-1 "General Principles for Technology Risk"[104]
- TM-G-2 "Business Continuity Planning"[105]
- PCPD Personal Data (Privacy) Ordinance (PDPO),[106] and accompanying Cloud Computing[107] and Outsourcing the Processing of Personal Data to Data Processors[108] information leaflets

Summary of market alignment with the recommendations

Regulatory Recommendations	Hong Kong's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**2 points: Cloud benefits generally acknowledged, no mention of public cloud.** HKMA notes in its 2018 consultation on draft guidelines for virtual banks that it does not object in principle to outsourcing of computer or business operations, including the use of external cloud services.[109] However, it has not specifically affirmed or promoted public cloud adoption.
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.** SA-2 requires FIs to conduct a risk assessment and perform appropriate due diligence to assess the ability of service providers before entering into an outsourcing arrangement.[110] It does not, however, offer specific guidance pertaining to cloud adoption.
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.** While FIs are not required to attain formal regulatory approval for outsourcing, those engaging in the outsourcing of banking-related business areas are required to discuss their outsourcing plans with the HKMA in advance.[111] This is, in effect, a 'de-facto' approval requirement where the result from the consultation will determine whether an FI is able to go ahead with the outsourcing activity.
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**2 points: Differentiation (materiality is defined) is made but same regulations apply to both material and non-material workloads.** There is no differentiation made in SA-2. TM-G-1 outlines additional controls that FIs are expected to implement in the outsourcing 'critical' technology services, such as commissioning a detailed assessment of the outsource provider's IT control environment and conducting annual assessments of the outsource provider's IT control environment. While data center operations are provided as an example, there is no clear definition of 'critical'.[112] In addition, there is also a requirement for virtual banks to discuss plans for material outsourcing with the HKMA in advance, but there is similarly no definition of materiality provided.[113]
5. Regulations should have a clear distinction between control vs processing of data	**6 points: Yes, there is a clear distinction between an entity that is a controller versus one that is a processor of data.** This distinction is made in the PDPC's Outsourcing the Processing of Personal Data to Data Processors information leaflet and referenced in the Cloud Computing information leaflet. The Cloud Computing information leaflet also clarifies that data users (or data controllers) are ultimately responsible

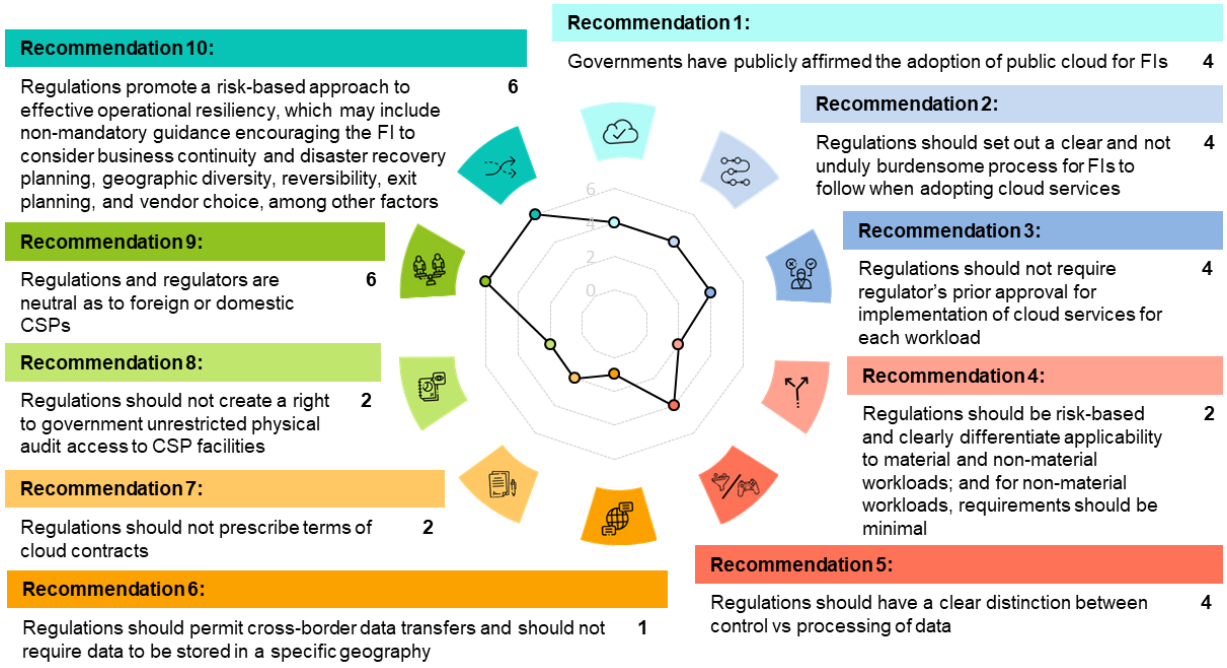
99 SFC, 31 October 2019, Circular to Licensed Corporations - Use of external electronic data storage, www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=19EC59 , although please note: The SFC subsequently released guidance on the circular, in the form of frequently asked questions (FAQs), which offers clarity to FIs' compliance obligations. Notably, the FAQ provides alternatives to the electronic data storage provider (EDSP) undertaking that is required under Section 7 of the Circular for the FI to exclusively keep regulatory records with a non-Hong Kong EDSP. SFC, 10 December 2020, SFC provides additional guidance on external electronic data storage, https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=20PR123
100 HKMA, https://www.hkma.gov.hk/eng
101 PCPD, https://www.pcpd.org.hk/
102 HKMA, Guideline on Authorization of Virtual Banks, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/guideline_eng_virtual_bank_20180608.pdf
103 HKMA, SA-2 "Outsourcing", http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
104 HKMA, TM-G-1 "General Principles for Technology Risk", http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf
105 HKMA, TM-G-2 "Business Continuity Planning", https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-2.pdf
106 PCPD, Personal Data (Privacy) Ordinance (PDPO), https://www.pcpd.org.hk/english/files/pdpo.pdf
107 PCPD, Cloud Computing information leaflet, https://www.pcpd.org.hk/english/resources_center/publications/files/IL_cloud_e.pdf
108 PCPD, Outsourcing the Processing of Personal Data to Data Processors information leaflet, https://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf
109 HKMA, Guideline on Authorization of Virtual Banks, Consultation Conclusions, https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180530e3a1.pdf
110 HKMA, SA-2, Sections 2.2 and 2.3, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
111 HKMA, SA-2 "Outsourcing", Section 1.3.2, http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
112 HKMA, TM-G-1, Section 7.1.1, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf
113 HKMA, Authorization of Virtual Banks, Section 23, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/guideline_eng_virtual_bank_20180608.pdf

Regulatory Recommendations	Hong Kong's Scores and Justifications
	for personal data collected and held by them and outsourcing of any processing or storage of personal data does not relieve them of this responsibility.[114] * "Data processor" is defined as "a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes".
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** While not yet in force, Section 33 of the PDPO in principle prohibits the cross-border transfer of personal data unless the individual's prior consent or other measures to ensure that the transfer destination offers the same protection as the PDPO have been taken. In practice however, organizations are only required to notify individuals of any intended transfers (overseas or otherwise) at the point of collection.[115] Nonetheless, FIs are advised to take the provisions of Section 33 into account when assessing their overseas outsourcing arrangements.[116] ACCA members observe that the HKMA has recently begun requesting for banking workloads to be stored onshore, which is in line with the ACCA's expectations that the SFC's data localization requirements would create a snowball effect on the broader financial industry.
b. Regulations should not require data to be stored in a specific geography	**1 point: No, only 'white listed' jurisdictions allowed.** SA-2 requires FIs that outsource a "major part" of its data processing function to outside Hong Kong to have a robust back-up system and contingency plan in an "acceptable jurisdiction".[117] FIs should also not outsource to a jurisdiction which is inadequately regulated or has secrecy laws that impede on access to data by the HKMA or FIs' external auditors.[118]
7. Regulations should not prescribe terms of cloud contracts	**6 points: Yes, regulations are not prescriptive as to terms of a cloud contract.** The only requirements laid out in SA-2 are that the outsourcing agreement clearly indicate the outsource provider's contractual liability and obligations, and that it includes a clause allowing for supervisory inspection of the outsource provider's operations and controls that relate to the outsourced activity.[119] The other regulatory requirements are presented as objectives.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no regulatory requirement of a right to unrestricted physical access for audit.** According to Section 2.8 of SA-2, FIs are required to ensure that they keep up-to-date records on-premise that are available for inspection by the HKMA, and that data retrieved from outsource providers are accurate and available in Hong Kong on a timely basis. Access to this data by the HKMA's examiners must not be impeded by the outsourcing arrangement, and this can be ensured by having a clause in the outsourcing which allows the HKMA to inspect or review the outsource provider's operations and controls.[120] This does not carry the expectation that HKMA requires unrestricted physical audit access to the CSP's premise.
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** SA-2 is clear in stating that "outsourcing can be to a service provider in Hong Kong or overseas".[121]
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** HKMA regulations promote a risk-based approach to contingency planning and are not prescriptive. As part of contingency planning, SA-2 suggests that FIs should consider, among other things, the availability of alternative service providers and possibility of bringing the outsourced activity back in-house.[122] As per TM-G-1, in addition to developing a contingency plan for critical outsourced technology services which "may include an exit management plan and the identification of additional or alternate technology service providers", FIs are instructed to "avoid placing excessive reliance on a single outside service provider in providing critical technology services".[123]

114 PCPD, Outsourcing the Processing of Personal Data to Data Processors information leaflet, https://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf; Cloud Computing information leaflet, https://www.pcpd.org.hk/english/resources_center/publications/files/IL_cloud_e.pdf
115 PCPD, PDPO, Section 33, https://www.pcpd.org.hk/english/files/pdpo.pdf
116 HKMA, SA-2, Section 2.9.1, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
117 HKMA, SA-2, Section 2.9.2, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
118 HKMA, SA-2, Section 2.9.1, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
119 HKMA, SA-2, Sections 2.5.1 and 2.8.2 https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
120 HKMA, SA-2, Section 2.8, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
121 HKMA, SA-2, Section 1.1.1, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
122 HKMA, SA-2, Section 2.7.3, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
123 HKMA, TM-G-1, Section 7.1.1, http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf

India

Figure 11: India's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 35

Market overview and key updates

Cloud adoption in India has accelerated in recent years, where the market is estimated to cross USD 7billion by 2022.[124] In the financial sector too, the transition to cloud is underway.

The Reserve Bank of India (RBI) maintains supervisory and inspection functions over all outsourcing arrangements and its regulations provide necessary guidance on adopting cloud. It is keenly aware of FIs adopting cloud in India and has acknowledged the benefits of cloud in key regulations as well. However, there is no cloud-specific guidance.

There are certain regulatory and policy initiatives that may prove challenging for CSPs. For instance, approvals are not required before outsourcing arrangements are made with overseas or domestic service providers, but banks are still required to report if the scale and nature of functions outsourced are significant, or extensive data is shared across geographies.[125] This contradictory, or unclear guidance may impair FI adoption of cloud.

There are also restrictions on cross-border transfers and storage for India. While not placing a bar on the processing of payment transactions outside India, RBI regulations stipulate that payments data can be stored only in India.[126]

Having said that, at present there are no explicit restrictions on foreign CSPs. For instance, the Ministry of Electronics and Information Technology (MeitY) provides accreditation (referred to as empanelment) of CSPs which enables them to be listed in the government cloud services directory, and allows government agencies

124 Economic Times, 2019, India's cloud market to cross $7 billion by 2022: Nasscom, https://economictimes.indiatimes.com/tech/internet/indias-cloud-market-to-cross-7-billion-by-2022-nasscom/articleshow/68689359.cms?from=mdr
125 RBI 2010-11/494, https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf
126 RBI, FAQs, Storage of Payment System Data, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130

to compare and procure cloud services easily.[127] The MeitY empanelment does not apply currently to FS regulated entities, but it is a process that could be brought to this sector.

RBI has also begun several initiatives to accelerate the development of India's FinTech industry, such as a regulatory sandbox for start-ups and FIs.[128] This allows safe live testing for products in different areas including retail payments and digital KYC, without the need for full regulatory approval.

Relevant regulator(s)

- Reserve Bank of India (RBI)[129]
- Ministry of Electronics and Information Technology (MeitY)[130]
- Department of Telecom (DoT)[131]

Relevant regulation(s)

- Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks[132]
- Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds[133]
- Cyber Security Framework in Banks[134]
- Guidelines on Sharing of IT Resources by Banks[135]
- Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of banks[136]
- Storage of Payment System Data[137]
- Credit Information Companies Regulations, 2006[138]
- Companies (Accounts) Rules, 2014[139]
- IDBRT FAQs on Cloud Adoption for Indian Banks[140]
- Personal Data Protection Bill 2019 (Draft)[141]
- National Cyber Security Policy, 2013[142]
- Information Technology Act, 2000[143]
- Information Technology (Amendment) Act 2008[144]
- Information Technology (Intermediaries Guidelines) Rules, 2011[145]
- [DRAFT] Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018[146]
- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[147]

Summary of market alignment with the recommendations

Regulatory Recommendations	India's Scores and Justifications
1. Governments have publicly affirmed the	**4 points: Benefits of public cloud acknowledged, but adoption not explicitly promoted.** The Information Security Guidelines state that public clouds allow high-availability systems to be developed at service levels often impossible to create in private

127 DoT, 2018, Availing Cloud Services From MeitY empanelled Cloud Service Providers, https://dot.gov.in/circulars/availing-cloud-services-meity-empanelled-cloud-service-providers
128 Business Standard, 2017, RBI finalises regulatory sandbox framework for innovation in fintech firms, https://www.business-standard.com/article/finance/rbi-finalises-regulatory-sandbox-framework-for-innovation-in-fintech-firms-119081400067_1.html
129 Reserve Bank of India, https://www.rbi.org.in/
130 Ministry of Electronics and Information Technology, https://www.meity.gov.in/
131 Department of Telecommunications, https://dot.gov.in/
132 RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
133 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
134 RBI 2015-16/418, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF
135 RBI, 2013-14/216, Guidelines on Sharing of IT Resources by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/CIRBMP03092013.pdf
136 RBI 2014-15/58, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/58MF300614FS.pdf
137 RBI 2017-18/153, Storage of Payment System Data, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF
138 RBI, 2006, Credit Information Companies Regulations, https://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf
139 MCA 2014, Companies (Accounts) Rules, https://www.mca.gov.in/Ministry/pdf/NCARules_Chapter9.pdf
140 IDRBT, 2017, FAQs on Cloud Adoption for Indian Banks, https://www.idrbt.ac.in/assets/publications/Best%20Practices/FAQ_Cloud.pdf
141 Personal Data Protection Bill, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
142 MCI, 2013, National Cyber Security Policy, https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf
143 MeitY, 2000, IT Act, https://www.meity.gov.in/writereaddata/files/itbill2000.pdf
144 MeitY, 2008, IT Act, Amendment, https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf
145 MeitY, 2011, Information Technology (Intermediaries Guidelines) Rules, https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf
146 MeitY, 2018, Information Technology (Intermediaries Guidelines) Rules, Amendment, https://www.prsindia.org/sites/default/files/bill_files/Draft_Intermediary_-Amendment_2018.pdf
147 MCI, 2011, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, https://www.wipo.int/edocs/-lexdocs/laws/en/in/in098en.pdf

Regulatory Recommendations	India's Scores and Justifications
adoption of public cloud for FIs	networks, except at extraordinary costs. The downside to this availability is the potential for commingling of information assets with other cloud customers, including competitors. Compliance with regulations and laws in different geographic regions can be a challenge for enterprises.[148]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to the cloud is not explicitly addressed, and/or processes are relatively burdensome.** What factors should be considered in due diligence and risk assessment are detailed in the IT Outsourcing Chapter of Information Security Guidelines[149] as well as the Outsourcing Guidelines.[150]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**4 points: Regulations do not require prior approval (or notice to the regulator and a letter of non-objection). However, in practice (either through verbal communication, as familiar practice, or out of an abundance of caution given the Information Security Guidelines), FSIs seek from RBI de facto approval / non-objection and thus, requirements are not clear.** Regulations do not require prior approval (or notice to the regulator and a letter of non-objection) Section 1.6(i) of the outsourcing guidelines clarifies that "Banks which desire to outsource financial services would not require prior approval from RBI whether the service provider is located in India or outside India." Outsourcing Guidelines state that banks that desire to outsource financial services would are not required to get prior approval from RBI whether the service provider is located in India or outside India[151] However, the Information Security Guidelines state that reporting to RBI is required when the scale and nature of functions outsourced are significant, or extensive data sharing is involved: Banks must be required to report to the regulator, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology / process outsourcing and when data pertaining to India[152]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**2 points: Differentiation (materiality is defined) is made but same regulations apply to both material and non-material workloads.** Outsourcing Guidelines state that during annual financial inspections, RBI will review the implementation of the Guidelines to assess the quality of related risk management systems particularly in respect to material outsourcing. Material outsourcing arrangements are those, that if disrupted have the potential to significantly impact business operations, reputation or profitability. Banks are encouraged to regularly review the materiality of their outsourced activities.[153] Some examples of outsourced activities that are material include technology operations, third party employees performing key banking functions such as applications processing, verifications, approvals etc.[154]
5. Regulations should have a clear distinction between control vs processing of data	**4 points: Draft regulation a makes distinction.** The [DRAFT] PDP Bill 2019 defines "data processor" as any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary; The "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;[155] As per the draft PDP Bill, consent is necessary for the processing of personal data. The Credit Information Companies Regulations, 2006 state that the credit information company is responsible for personal data in its possession or custody, including information that has been transferred to a third party for processing. The credit information company shall use contractual and other means to provide a comparable level of protection while the information is being processed by a third party.[156]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**1 point: Not allowed, with some exceptions.** As per the Storage of Payment System Data, and subsequent clarifications by RBI, *there is no bar on processing of payment transactions outside India*. However, the data shall be stored only in India after the processing. The complete end-to-end transaction details should be part of the data. In case the processing is done abroad, the data should be deleted from the systems abroad and brought back to India not later than the one business day or 24 hours from payment processing, whichever is earlier. The same should be stored only in India.[157]
b. Regulations should not require data to be stored in a specific geography	**0 points: Data must be stored in specific geographic locations.** The Storage of Payment System Data states that all system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details/information collected/carried/processed as part of the message/payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign jurisdiction, if required.[158] In the case of banks, especially foreign banks, earlier specifically permitted to store the banking data abroad, they may continue to do so; however, in respect of domestic payment transactions, the data shall be stored only in India, whereas for cross border payment transactions, the data may also be stored abroad as indicated earlier.[159] The current draft of the PDP Bill 2019 includes financial data in 'sensitive personal data'. Sensitive personal data may only be transferred outside of India for the purpose of processing, but such sensitive personal data shall continue to be stored in India. (Clause 33 and 34).[160] It is not entirely in line with the RBI guidelines.

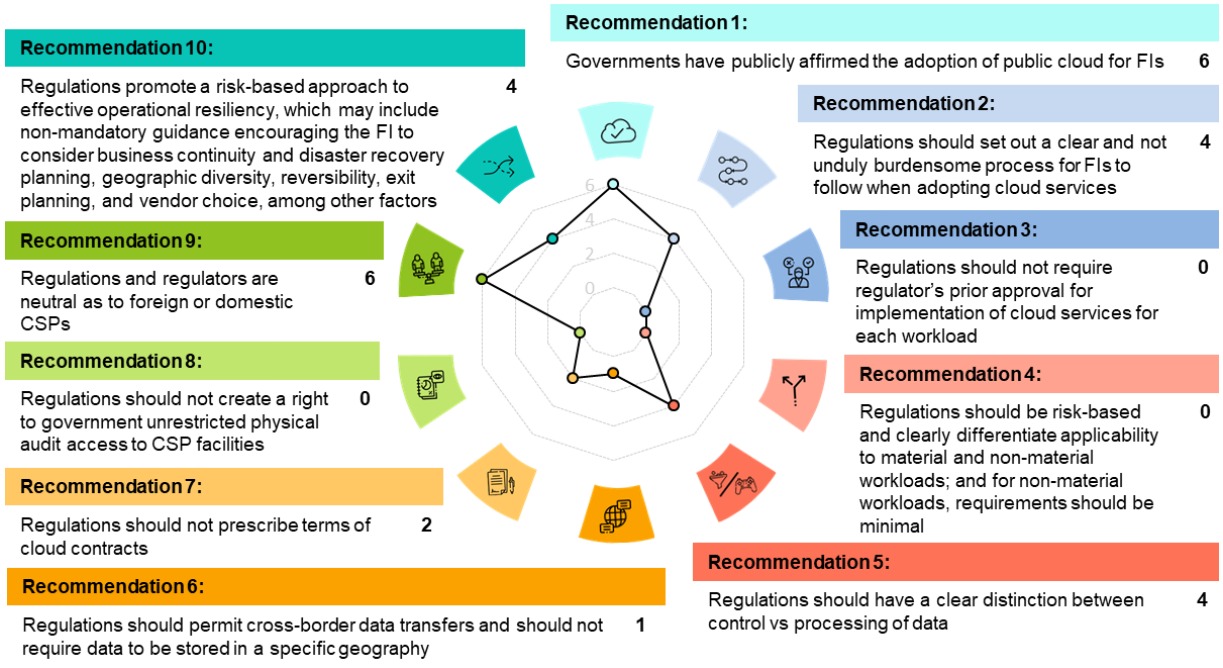
148 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
149 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
150 RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
151 RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
152 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
153 RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
154 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
155 Personal Data Protection Bill, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
156 RBI, 2006, Credit Information Companies Regulations, https://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf
157 RBI, FAQs, Storage of Payment System Data, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130
158 RBI 2017-18/153, Storage of Payment System Data, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF
159 RBI, FAQs, Storage of Payment System Data, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130
160 Personal Data Protection Bill, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Regulatory Recommendations	India's Scores and Justifications
7. Regulations should not prescribe terms of cloud contracts	**2 points: Regulations have overly detailed requirements for the cloud contract, but do not go to the extent of prescribing specific contractual language.** Outsourcing Guidelines[161] contain a lot of detail on what should be included. For instance, outsourcing agreements should include clauses to allow RBI or persons authorised by it to access the bank's documents, records of transactions etc; and also include a clause to allow for an inspection to be made of a service provider of a bank and its books and accounts. Information Security Guidelines also highlight the areas that '*should*' be covered in the contractual agreements in great detail. These relate to scope, performance standards, audit and inspection, termination clauses, business continuity etc.[162] It is also stated that recovery team objectives should be stated in the contract.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**2 points: It is not clear if regulations require the CSP to provide the regulator with unrestricted physical access.** Information Security Guidelines state contractual agreements should include provisions for access to books and records/audit and inspection. Banks should have the ability to access all books, records, and information relevant to the outsourced activity available with the service provider. The bank should also have the right to conduct audits on the service provide by its internal or external auditors, or by external specialists, and to obtain copies of any audit or review reports and findings made on the service provider in relation to the outsourced activities. However, the Guidelines also add that the Reserve Bank has the right to cause an inspection to be made of a service provider of a bank and its books and accounts by one or more of its officers or employees or other persons. [163]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** There are no explicit restrictions on foreign CSPs. MeitY provides accreditation (referred to as empanelment) of CSPs which enables them to be listed in the government cloud services directory, and allows government agencies to compare and procure cloud services easily.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** In the Outsourcing Guidelines, key risks that the bank must evaluate are highlighted. Exit Strategy Risk – This could arise from over–reliance on one firm, the loss of relevant skills in the bank itself preventing it from bringing the activity back in-house and contracts entered wherein speedy exits would be prohibitively expensive.[164] The Outsourcing Guidelines further state that in establishing a viable contingency plan, banks should consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency and the costs, time and resources that would be involved. In Sharing of IT Resources by Banks Guidelines, it is recommended that portability and interoperability be analyzed. This would involve considering factors necessitating switching service providers, negotiating contract price increase, factoring in service provider bankruptcy and service shutdown, decrease in service quality and business disputes.[165] The Information Security Guidelines discuss Multiple Service Provider relationships. A multiple service provider relationship is one where two or more service providers collaborate to deliver an end to end solution to the financial institution. Multiple contracting scenarios are possible: • One service provider may be designated as the 'Lead Service Provider', to manage the other service providers. • Bank may independently enter into stand-alone contracts with each service provider. An institution selects from the above or any other contractual relationship, however, remains responsible for understanding and monitoring the control environment of all service providers that have access to the banks systems, records or resources.[166]

161 RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
162 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
163 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf and RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
164 RBI, 2006/167, Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF
165 RBI, 2013-14/216, Guidelines on Sharing of IT Resources by Banks, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/CIRBMP03092013.pdf
166 RBI 2010-11/494, Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf

Indonesia

Figure 12: Indonesia's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 27

Market overview and key updates

In general, Indonesia's banking regulator OJK promotes the adoption of digital technologies by FIs. This is in line with President Joko Widodo's policy of promoting digital economy growth,[167] which has seen the Indonesian government adopting national frameworks such as 2020 Go Digital Vision and Industry 4.0 Roadmap that is driving the digitalization of Indonesian businesses.

Since our 2018 report, OJK has also issued new technology-centric regulations such as Regulation No.12/POJK.03/2018, which regulates commercial bank's provision of digital banking services, and Regulation No.13/POJK.02/2018, which regulates FinTech, reflecting an increased appetite for digital technologies and services by Indonesian FIs and their customers. In August 2020, OJK made public that it is preparing terms for the issuance of digital bank licenses in response "to the digitalization needs of the Indonesian financial services industry",[168] and issued its Digital Finance Innovation Road Map and Action Plan 2020-2024 to support the development of the digital financial innovation ecosystem by balancing the facilitation of digital financial innovation with strong financial consumer protection and supervisory frameworks.[169]

The most significant implications for the cloud in OJK's recent spate of supportive regulations is unarguably Regulation No. 13/POJK.03/2020, which revises Regulation No. 38/POJK.03/2016 Risk Management in Use of Information Technology by Commercial Banks, relaxing some of the data localization requirements contained in Article 21 of the original 2016 regulation (see 6 b. of Summary of market alignment with the

167 OJK, 17 March 2016, Press Release: OJK Encourages Banks to Optimize Digital Services, https://www.ojk.go.id/en/kanal/perbankan/berita-dan-kegiatan/siaran-pers/Pages/Press-Release-OJK-Encourages-Banks-to-Optimize-Digital-Services.aspx
168 Kontan.co.id, 22 August 2020, OJK has prepared digital bank license terms to respond to industry needs, https://keuangan.kontan.co.id/news/ojk-siapkan-ketentuan-lisensi-bank-digital-untuk-merespons-kebutuhan-industri
169 OJK, 31 August 2020, Digital Finance Innovation Road Map and Action Plan 2020-2024, https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Pages/Publikasi-Materi-Digital-Finance-Innovation-Road-Map-dan-Action-Plan-2020-2024-serta-Digital-Financial-Literacy.aspx

recommendations section for details). While this change has been well-received by the FIs and CSPs alike, regulations are still restrictive of cross-border data transfers as Indonesian FIs are only allowed to store data overseas for limited functions which have to be pre-approved by the OJK. Nonetheless, recent developments in national regulations show Indonesia's increasingly open stance on cross-border data transfers, providing impetus for remaining regulatory barriers to be removed and for the advancement of FIs' use of cloud:

- **GR 71/2019 on the Implementation of Electronic Systems and Transactions**[170] took effect on 10 October 2019, replacing GR 82/2012, which had been criticized for its restrictive approach to data transfers that inhibits cloud adoption. GR71/2019 introduces an important distinction between private and public sector electronic service providers (ESPs), and allows private sector ESPs to store data overseas, although local registration is still required. Importantly, GR71/2019 does not apply to the public financial services institutions, while private financial services institutions are still required to defer to OJK/BI regulation on data location. That said, GR 71/2019 signifies a greater understanding and receptiveness toward cloud computing and cross-border data transfers at the broader national level, and the new and more relaxed conditions for the cross-border transfer of personal data provided by Regulation No. 13/POJK.03/2020 appears to be an effort by the OJK to align sectoral regulation with this new stance.
- While the discussion has been underway since 2012, Indonesia has yet to enact a personal data protection law. However, Kominfo officially submitted the **draft RUU PDP** to the House of Representatives in January 2020, and announced in May that the House of Representatives would commence discussions on the Draft Law on Personal Data Protection (RUU PDP) in June. Kominfo noted that discussions, which were initially outlined to begin in March, were delayed due to the onset of the COVID-19 pandemic.[171] The RUU PDP is on the country's 2020 Priority National Legislation Program and is targeted for completion in November 2020.[172] When enacted, the RUU PDP will draw a clear distinction between personal data processors and controllers, and allow personal data controllers to transfer data overseas. Unlike GR71/2019, the scope of the RUU PDP covers personal financial data and does not provide for deference to sectorial regulation. There is therefore a strong likelihood that the enactment of RUU PDP spurs OJK to undertake a renewed review of sectoral regulation so that the RUU PDP's conditions for cross-border transfers of personal financial data may be applied uniformly across the FSI (and not just for specific FI functions).

OJK permits the use of cloud computing by FIs, and although it has not made official statements to recognize the benefits of the cloud and publicly promote it, ACCA members' experience suggests that OJK is supportive of FIs' use of the cloud. However, there remains a major regulatory limitation in advancing the use of cloud in the form of Regulation No. 9/POJK.03/2016, which prevents banks from outsourcing 'main work' (see 'Summary of market alignment with the recommendations'). As Indonesian FIs' use of cloud and other digital technologies mature, a review of such regulatory obstacles may be necessary.

Relevant Regulator(s)

- Financial Services Authority of Indonesia (OJK)[173]
- Ministry of Communication and Informatics (Kominfo)[174]

170 Kominfo, 10 October 2019, Government Regulation Number 71 of 2019, https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019
171 Indotelko, 25 May 2020, The PDP Bill will begin to be discussed next June, https://www.indotelko.com/read/1590382148/ruu-pdp-juni
172 Indotelko.com, 7 September 2020, The discussion on the PDP Bill is expected to be completed in November, https://www.indotelko.com/read/1599431680/pembahasan-november
173 OJk, https://www.ojk.go.id/Default.aspx
174 Kominfo, https://www.kominfo.go.id/

Key Regulation(s)

- Regulation No. 38/POJK.03/2016[175] and its amendment Regulation No. 13/POJK.03/2020[176], Circular Letter 21/SEOJK.03/2017[177] on Risk Management in Use of Information Technology by Commercial Banks
- Regulation No. 9/POJK.03/2016 concerning the Principle of Prudence for Commercial Banks Submitting Part of Their Work Implementation to Other Parties[178]
- (Draft) Personal Data Protection Law (RUU PDP)[179] (December 2019)

Summary of market alignment with the recommendations

Regulatory Recommendations	Indonesia's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**6 points: Yes, public cloud adoption is promoted in a public affirmation.** OJK permits the use of cloud computing by FIs[180] and based on ACCA members' experience, is supportive of the use of public cloud. OJK also generally promotes the adoption of digital technologies by FIs, which is in line with President Joko Widodo's policy of promoting digital economy growth.[181]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.** While Indonesia does not have a specific guideline/checklist for adopting cloud, Section 2.3.1 of Circular No. 21/SEOJK.03/2017 offers guidance across 9 stages of IT outsourcing that can also be referenced for cloud adoption.
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.** According to Regulation No. 38/POJK.03/2016, Commercial banks planning to operate an electronic system outside Indonesia are required to submit an application to the OJK for approval three months before the arrangement starts. In addition, FIs that plan to outsource the operation of their data centers/ disaster recovery centers/ IT-based transaction processing to a service provider in Indonesia must notify the OJK of this at least two months before the arrangement starts. Moreover, FIs are also required to report the realization of the outsourced activity to the OJK within one month from when the outsourced activities commence.[182]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**0 points: No differentiation and all workloads are treated equally.** According to Regulation No. 9/POJK.03/2016, commercial banks are only allowed to outsource work classified as 'support work' which is defined as activities that are (i) low risk; (ii) do not require high banking competency and skills qualification; and (iii) do not directly relate to operational decision-making. 'Main work' which, if unavailable, would be disruptive to the FI's functioning, cannot be outsourced.[183] All workloads that can be outsourced are subject to the same regulatory requirements.
5. Regulations should have a clear distinction between control vs processing of data	**4 points: Draft regulation makes distinction.** This distinction is made in the current draft of the RUU PDP.[184]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**1 point: Not allowed, with some exceptions.** While personal data can now be transferred overseas in some specific situations and with OJK's prior approval, as elaborated in 6 b., restrictions still exist and OJK requires FIs' data centers and disaster recovery centers to be located within Indonesia. However, Article 23 of Regulation No. 38/POJK.03/2016 states that the *information technology-based transaction processing* can be carried out by service providers outside Indonesia, but subjects the FI to a few additional requirements – such as attaining prior approval from OJK and demonstrating efforts to develop the Indonesian economy – in addition to fulfilling the same set of conditions as the required of FIs undertaking transaction processing domestically.[185]

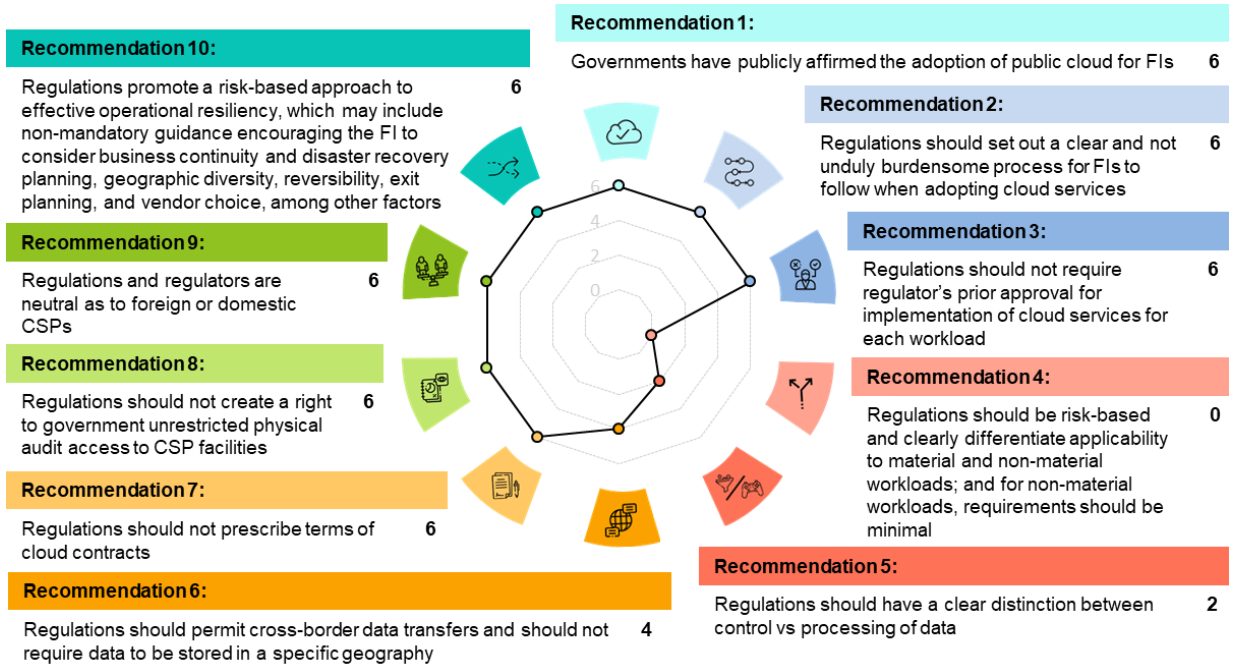
175 OJK, Regulation No. 38/POJK.03/2016, http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf
176 OJK, Regulation No. 13/POJK.03/2020, https://ojk.go.id/id/regulasi/Pages/tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx
177 OJK, Circular Letter 21/SEOJK.03/2017, https://www.ojk.go.id/id/regulasi/Pages/SEOJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx
178 OJK, Regulation No. 9/POJK.03/2016, https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Pages/pojk-prinsip-kehatian-bank-umum-yang-melakukan-penyerahan-sebagian-pelaksanaan-kerja-kpd-pihak-lain.aspx
179 Kominfo, (Draft) Personal Data Protection Law (RUU PDP), https://kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers
180 Indotelko, 23 December 2016, ICCA is waiting for OJK regulations regarding Cloud in the financial industry, https://www.indotelko.com/read/1482453280/icca-keuangan
181 OJK, 17 March 2016, Press Release: OJK Encourages Banks to Optimize Digital Services, https://www.ojk.go.id/en/kanal/perbankan/berita-dan-kegiatan/siaran-pers/Pages/Press-Release-OJK-Encourages-Banks-to-Optimize-Digital-Services.aspx
182 OJK, Regulation No. 38/POJK.03/2016, Article 24, http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf
183 OJK, Regulation No. 9/POJK.03/2016, Articles 4(3) and 5, https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Pages/pojk-prinsip-kehatian-bank-umum-yang-melakukan-penyerahan-sebagian-pelaksanaan-kerja-kpd-pihak-lain.aspx
184 Kominfo, Draft RUU PDP, Article 1, https://kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers
185 OJK, Regulation No. 38/POJK.03/2016, Article 23, http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf

Regulatory Recommendations	Indonesia's Scores and Justifications
	It is at the moment unclear how the RUU PDP – if passed in its current draft form – will be implemented for the financial services sector since the draft RUU PDP allows personal data controllers to transfer personal data (including personal financial data) outside Indonesia if: (i) the country has a level of protection equal to or exceeding that in Indonesia; (ii) there are international agreements between countries; (iii) there is a contract between the data controllers guaranteeing data protection in accordance with Indonesian law; and/or (iv) the data controller has obtained the approval of the data subject.[186]
b. Regulations should not require data to be stored in a specific geography	**0 points: Data must be stored in specific geographic locations.** By default, FIs are required to use data centers and disaster recovery centers located in Indonesia. However, there are some key exceptions to this rule as provided for in Article 21 (2) and (3) of Regulation No. 38/POJK.03/2016, amended as per Regulation No. 13/POJK.03/2020. Subject to OJK's approval, FIs may place their electronic systems in data centers and/ or disaster recovery centers outside of Indonesia in specific circumstances: where they are required to support integrated analysis; for risk management and AML/CTF functions of overseas-headquartered banks; to provide services to customers globally; to facilitate communication management between offices; and for internal management purposes. provided that the data involved does not contain personally identifiable customer information.[187] While the amended Article 21 relaxes some of the previous restrictions on the overseas transfer of personally identifiable customer information for the above functions and allows for *front-end* electronic systems that provide services to a global customer base to be stored in data centers and disaster recovery centers outside Indonesia, it also makes clear that commercial banks must still store their back-end systems that process personal data, accounts and/or transactions locally.[188]
7. Regulations should not prescribe terms of cloud contracts	**2 points: Regulations have overly detailed requirements for the cloud contract, but do not go to the extent of prescribing specific contractual language.** Section 9.2.2 of Circular No. 21/SEOJK.03/2017, which describes the contents of the minimum standard for an outsourcing agreement with an IT service provides, and contains some general requirements (e.g. scope of work, cost and duration of agreement, security standards), but also some specific requirements (e.g. HR training plan, both the number trained, the form of training and the costs required).[189] However, it does not prescribe specific contractual language.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**0 points: Regulations specify that unrestricted physical access is required.** According to Section 9.2.2 of Circular No. 21/SEOJK.03/2017, commercial banks must, for audit purposes, allow both the commercial bank's internal auditors, the OJK, and/ or external auditors appointed by the commercial bank or OJK to have both logical and physical access rights to inspect information managed by the outsource service provider.[190] This suggests that there are no limit to OJK's physical access rights.
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** OJK does not offer preferential treatment of domestic CSPs. According to Circular No. 21/SEOJK.03/2017, "similar to the use of domestic IT service providers, the use of IT services from foreign parties or those located outside the territory of Indonesia must go through the same procedure". That said, the use of IT service providers outside the territory of Indonesia is subject to prior approval from the OJK.[191]
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**4 points: Regulations promote a risk-based approach to operational resiliency and are not prescriptive, but do not include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.** Circular No. 21/SEOJK.03/2017 guides to FIs on taking risk-based approaches to issues around issues of operational resiliency. For example, the circular notes that the outsourcing agreement must contain a specific clause stating the possibility of changing, making new agreements, or taking over activities carried out by the IT service provider or terminating the agreement before the end of the agreement. In addition, Section 3.2.5 c) on 'Data migration' indicates that FIs need to have policies, standards and procedures to handle data migration across different systems as part of its change management policy, and Section 4.3.1 b. 3 c) states that FIs should have backup facilities that 'have different risks with the main equipment, such as using a different service provider'. FIs are also encouraged to ensure compatibility and interoperability as a risk control measure in Section 2.2b.[192]

186 Kominfo, Draft RUU PDP, Article 49, https://kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers
187 OJK, Regulation No. 38/POJK.03/2016, Article 21(2), http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf
188 OJK, Regulation No. 13/POJK.03/2020, Article 1(3), https://ojk.go.id/id/regulasi/Pages/tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx
189 OJK, Circular No. 21/SEOJK.03/2017, Section 9.2.2 c., https://www.ojk.go.id/id/regulasi/Pages/SEOJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx
190 OJK, Circular No. 21/SEOJK.03/2017, Section 9.2.2, https://www.ojk.go.id/id/regulasi/Pages/SEOJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx
191 OJK, Circular No. 21/SEOJK.03/2017, Section 9.2.3 g., https://www.ojk.go.id/id/regulasi/Pages/SEOJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx
192 OJK, Circular No. 21/SEOJK.03/2017, Various Sections, https://www.ojk.go.id/id/regulasi/Pages/SEOJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum.aspx

Japan

Figure 13: Japan's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 48

Market overview and key updates

The Japanese cloud services market is expected to grow at 18% CAGR to USD18billion by 2023.[193] One of the key drivers of this growth is the government's encouragement and adoption of the cloud through its 'cloud by default' policy. In the financial sector, cloud adoption is also increasing, and financial institutions use it most commonly for data analysis, risk modelling, and customer services, and more recently core banking systems as well.

The main regulator in the financial sector, FSA, does not have cloud-specific regulations, but guidance is available to financial institutions through the Comprehensive Guidelines for Supervision of Major Banks.[194] Guidelines are also published by FISC, which provides more detailed and specific guidance related to cloud computing. The regulatory and policy approach is generally conducive to cloud adoption in the financial sector, with very specific guidance offered on key issues relating to data security and protection. For instance, the FISC Guidelines mandate that data provided by financial institutions be erased in an appropriate manner and time frame; information linking the data management area and data storage area be severed; and that the data storage area be wiped.

In recent years, the government has enhanced the legal and regulatory landscape to push for financial innovation e.g. it made changes to the Banking Act and made it easier for FIs to offer services using APIs.[195] In 2017, the FSA introduced the 'FinTech Testing Hub' to support FIs with emerging risks and legal issues.[196]

193 BCG, 2019, Japan Market Report https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/japan
194 FSA, 2 Jul 2014, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
195 Brink, 2018, How Japan's Open API Adoption Could Change Financial Institutions in the Region, https://www.brinknews.com/how-japans-open-api-adoption-could-change-financial-institutions-in-the-region/
196 Nikkei, Asian Review, 2017, Japan to establish fintech testing 'hub', https://asia.nikkei.com/Business/Finance/Japan-to-establish-fintech-testing-hub

The regulatory sandbox scheme was introduced in 2018 and looks to promote fintech in several areas including blockchain, AI, and IoT.[197]

Relevant regulator(s)

- Financial Services Agency (FSA)[198]
- The Center for Financial Industry Information Systems (FISC)[199]

Relevant regulation(s)

- Banking Act[200]
- Comprehensive Supervision Guidelines for major banks[201]
- Guidelines for Personal Information Protection in the Financial Field[202]
- Act on Protection of Personal Information (APPI)[203]
- Report of the Council of Experts on Outsourcing in Financial Institutions (FISC) – 2016 version[204]
- Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions (FISC) – 2014 version[205]
- Security Guidelines on Computer Systems for Banking and Related Financial Institutions (FISC) – 9th version June 2019[206]

Summary of market alignment with the recommendations

Regulatory Recommendations	Japan's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**6 points: Yes, public cloud adoption is promoted in a public affirmation.** The Comprehensive Guidelines for Supervision of Major Banks note that when banks entrust business operations to third-party entities (outsourcing), they can enhance management efficiency. Moreover, by entrusting business operations to entities with superior expertise, banks can expect better response to diverse needs of customers, and prompt actions based on quick technological innovation.[207] Japanese government's announcement in 2018 that it was embarking on a 'cloud by default' policy is a key driver. Government agencies procuring new IT for their applications consider public cloud as the first option, then private cloud, and then on-premises storage solutions.[208]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**6 points: Yes, regulations set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption (could be through a reference in the regulation itself or in accompanying cloud computing guidelines/ information papers). Such processes are proportionate, practical and not unduly burdensome.** The Comprehensive Guidelines for Supervision of Major Banks requires banks to select contractors by examining the capability of providing service at a sufficient level, financial and management conditions to provide services and pay for any damages, and any reputational issues for the bank.[209]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**6 points: No regulator's approval necessary – (compliance with global standards and international third-party certifications are sufficient).** No regulatory notification or approval is required for outsourcing transactions.
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**0 points: No differentiation and all workloads are treated equally.** Material and Non-material workloads are not described clearly. The Comprehensive Guidelines for Supervision of Major Banks only define "Outsourcing" and explain that it includes entrustment of administrative operations necessary for operating business. Cases where a business operation is deemed to be virtually outsourced without the signing of an outsourcing contract, and cases where the outsourced business operation is conducted abroad, are also included. It does not include entrusting the business management or the function of operational management (including important personnel management policies) to an external entity.[210]

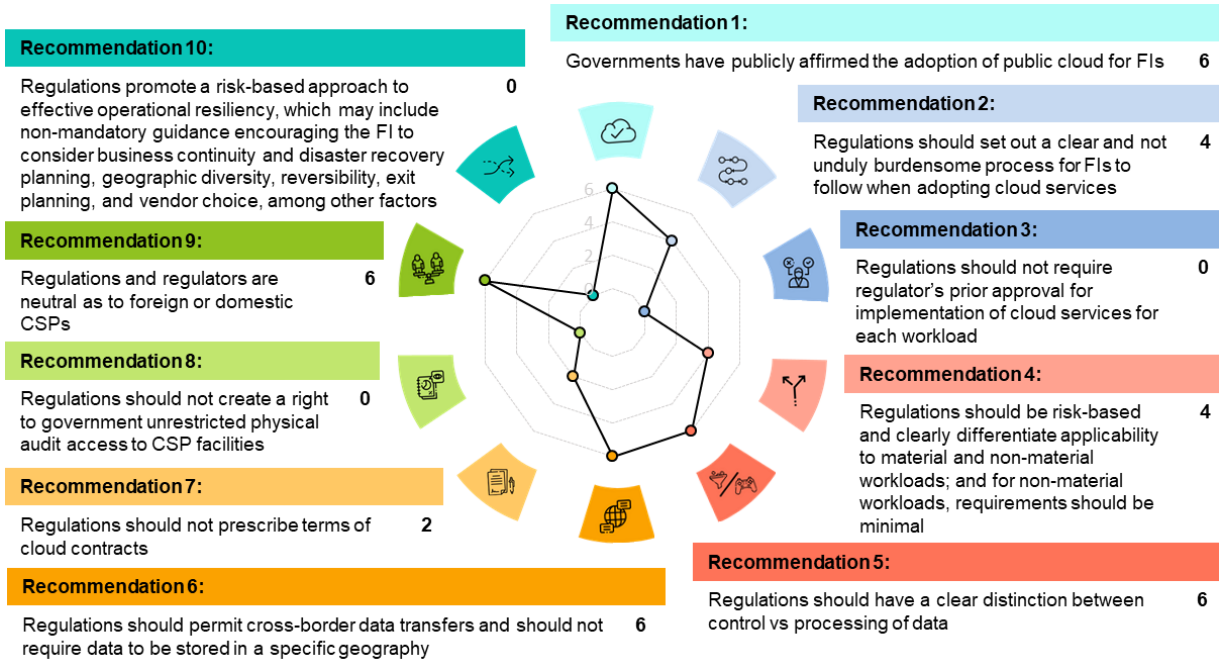
197 JETRO, n.d., New Regulatory Sandbox framework in Japan, https://www.jetro.go.jp/ext_images/en/invest/incentive_programs/pdf/Detailed_overview.pdf
198 Financial Services Agency, https://www.fsa.go.jp/en/
199 Center of Financial Industry Information Systems, https://www.fisc.or.jp/english/
200 Banking Act, http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=2&dn=1&x=53&y=23&co=0-1&ia=03&ja=04&ky=banking+act&page=6
201 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
202 FSA, Guidelines for Personal Information Protection in the Financial Field https://www.fsa.go.jp/frtc/-kenkyu/event/20070424_02.pdf
203 PPC, Act on Protection of Personal Information (APPI), https://www.ppc.go.jp/en/
204 FISC, 2016, Report of the Council of Experts on Outsourcing in Financial Institution, https://www.fisc.or.jp/-data/english/pdf/FISC_Outsourcing_Report_2016.pdf
205 FISC, 2014, Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions, https://www.fisc.or.jp/data/english/pdf/FISC_Cloud_Report-_2014.pdf
206 FISC, Security Guidelines, https://www.fisc.or.jp/english/
207 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
208 BCG, 2019, Japan Market Report https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/japan
209 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
210 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf

Regulatory Recommendations	Japan's Scores and Justifications
5. Regulations should have a clear distinction between control vs processing of data	**2 points: Unclear or ambiguous (e.g. mentions but no definition).** There is no concept of 'data controller' or 'data processor' in the APPI. It uses the term 'business operator' which refers to the entity responsible for the proper handling of all "Personal Information." A business operator shall not handle personal information beyond the scope necessary for achieving the purpose of use unless it has obtained prior consent of data subjects, and accountability also lies with business operator.
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** Cross border transfer of data is allowed, but requires consent of the data subject, prior to the transfer; the country in which recipient is located has a legal system equivalent to Japanese personal data protection; and recipient takes adequate precautionary measures for the protection of personal data.[211]
b. Regulations should not require data to be stored in a specific geography	**1 point: No, only 'white listed' jurisdictions allowed.** In the APPI it is mentioned that the foreign country receiving the data must have substantially similar standards as the APPI. For this purpose the PPC has implemented a framework to identify the foreign countries with adequate measures (adequacy list) on personal data. In 2019, the EU (including the UK) was included in the adequacy list. Reciprocally, the European Commission also identified Japan in the Commission Implementing Decision (EU) 2019/419 of 23 January 2019. UK is on the list post-Brexit.[212]
7. Regulations should not prescribe terms of cloud contracts	**6 points: Regulations are not prescriptive as to terms of a cloud contract.** Comprehensive Guidelines for Supervision of Major Banks mention the content of contracts. Contracts should include the contents and level of service to be provided, and the procedures for cancellation; responsibility of the outsourcing contractor when the service is not provided as specified under contract, as well responsibility of payment of damages that may arise with regard to the outsourcing, including the provision of collateral; contents of the reports that the bank would receive from the outsourcing contractor; and arrangements concerning how to meet requests from the financial authority in relation to inspection and supervision.[213] (FISC), Security Guidelines on Computer Systems for Financial Institutions, Section V-2(1) No. 21 (9th Edition, 2018), mandate the inclusion of several contract provisions relating to ongoing oversight, such as provisions requiring cloud providers to disclose information to a financial institution in the event of increased risk of information leakage or in the event the cloud provider's internal controls have weakened.[214]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports.** As per the Comprehensive Guidelines for Supervision of Major Banks the outsourced business operation is subject to audits.[215] FISC recommends Financial Institutions leverage reports from assurance audits consigned by the cloud service provider, such as SOC 1 and SOC 2 reports, when conducting audits.
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** No evidence of preferential treatment for domestic CSPs or additional requirements for foreign CSPs.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**6 points: Regulations promote a risk-based approach to operational r esiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** As per the Comprehensive Guidelines for Supervision of Major Banks, it will be checked if banks have undertaken risk management. This includes banks conducting comprehensive verification of various risks related to outsourcing, such as the impact that may be inflicted on the banking business if it fails to receive services as specified under the contract, and what actions to taken when such risks materialize.[216] Guidelines published by FISC provide detailed, specific requirements regarding termination of cloud services. They provide that outsourcing contracts must address exit procedures and responsibilities, by including provisions requiring the cloud provider to facilitate the extraction of data that will be transferred to a new cloud provider or an existing in-house system and allocating the burden of transfer expenses in different scenarios. The guidelines also include instructions for protecting data upon termination, mandating that: data provided by financial institutions be erased in an appropriate manner and time frame; information linking the data management area and data storage area be severed; and that the data storage area be wiped.[217]

211 PPC, Act on the Protection of Personal Information, https://www.ppc.go.jp/en/
212 PPC, Act on the Protection of Personal Information, https://www.ppc.go.jp/en/
213 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
214 PIFS, 2019, Cloud Computing in the Financial Sector: A Global Perspective, https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf
215 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
216 FSA, Comprehensive Supervision Guidelines for major banks, https://www.fsa.go.jp/common/law/guide/gaigin.pdf
217 PIFS, 2019, Cloud Computing in the Financial Sector: A Global Perspective, https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf

Malaysia

Figure 14: Malaysia's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 34

Market overview and key updates

With FIs moving towards greater adoption of technology, Bank Negara Malaysia (BNM) has responded by drawing up regulatory requirements and guidelines for outsourcing arrangements. It issued an exposure draft in September 2017 to obtain public and industry feedback. Thereafter the policy document on Outsourcing was released focusing mainly on the management of outsourcing risk and governance standards to be enforced by the FI's board and senior management, due diligence in selecting service providers, and protection of data and business continuity planning.[218]

As security remains a chief concern for BNM, the regulatory processes are more conservative and protective, and FI's must obtain written approval before entering new material outsourcing arrangements or making significant modifications to existing outsourcing arrangements such as change in CSP or change of country location. Outsourcing plans for the financial year must also be submitted by the FI prior to submission of outsourcing applications.

BNM has also updated the Risk Management in Technology (RMiT) guidelines in June 2020 to indicate minimum standards in the management of technology risk exposure.[219] In a positive development, BNM only needs to be notified about use the of cloud for non-critical systems, with prior approval only required for critical systems. Overall, BNM has adopted a more open and forthcoming approach towards cloud adoption in the financial sector.

In order to encourage innovation in the financial sector, BNM also introduced its regulatory sandbox in 2016 to enable firms to test innovative solutions. The insights gained from this process have led to BNM adapting

218 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
219 BNM, Jun 2020, Risk Management in Technology (RMiT), https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078

existing regulations as well as developing a licensing framework for digital banks.[220] BNM has also introduced regulations on electronic Know-Your-Customer to enable the secure adoption of e-KYC technology in the financial sector[221], and set out a policy document on the development and publication of Open API.[222]

Most recently, it has collaborated with the Malaysia Digital Economy Corporation (MDEC), to support the growth and development of fintech companies through the Fintech Booster programme.[223] The programme will help companies develop products and services by enhancing their understanding of legal and regulatory requirements, and facilitate innovation in the financial services sector.

Relevant regulator(s)

- Bank Negara Malaysia (BNM)[224]
- Department of Personal Data Protection (JPDP)[225]

Relevant regulation(s)

- Risk Management in Technology 2020 (RMiT)[226]
- Policy Document on Outsourcing 2019 (supersedes Policy Document on Outsourcing issued on 28 Dec 2019)[227]
- Personal Data Protection Act (PDPA) 2010[228]
- Guidelines on Data Management and MIS Framework[229]
- Management of Customer Information and Permitted Disclosures[230]
- Business Continuity Management (Revised)[231]
- Financial Services Act 2013[232]

Summary of market alignment with the recommendations

Regulatory Recommendations	Malaysia's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**6 points: Yes, public cloud adoption is promoted in a public affirmation.** The Malaysian government stated its intention of increasing cloud adoption in the public sector in 2017. While it, as yet, does not have a cloud-first policy in place, it has most recently set a target of achieving 50% cloud adoption by the year 2024. In 2021 it will focus on the implementation of this strategy in the public sector.[233] More recently, BNM has adopted a more open and forthcoming stance towards cloud adoption in the financial sector, offering greater clarity through various regulations. In the most recently Outsourcing Policy document, it has also acknowledged that financial institutions are increasing the use of cloud services to improve business agility in responding to customer needs and achieving economies of scale. [234]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.** In the Outsourcing Policy Document, it is recommended that comprehensive and robust due diligence process be undertaken, to make an informed selection of service providers, in relation to the risks associated with the outsourcing arrangement. What should be covered in the due diligence exercise is made mandatory.

220 BNM, December 2020, Licensing Framework for Digital Banks, https://www.bnm.gov.my/documents/20124/938039/20201231_Licensing+Framework+for+Digital+Banks.pdf
221 BNM, June 2020, e-KYC, https://www.bnm.gov.my/documents/20124/883228/e-KYC+Policy+Document+300620.pdf
222 BNM, January 2019, Publishing Open Data using Open API, https://www.bnm.gov.my/documents/20124/761679/Open+Data+API+PD.pdf
223 BNM, August 2020, Press Release, Launch of the Fintech Booster Programme, https://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=5089
224 Bank Negara Malaysia, https://www.bnm.gov.my/
225 Department of Personal Data Protection, https://www.pdp.gov.my/jpdpv2/?lang=en
226 BNM, June 2020, Risk Management in Technology, https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078
227 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
228 Personal Data Protection Act, 2010, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf
229 BNM, 2011, Guidelines on Data Management and MIS Framework, https://www.bnm.gov.my/documents/20124/938039/PD+Management+of+Customer+Info.pdf/0822334e-95b2-0cd9-ecdc-1fbf275a27a2?t=1592247605654%27
230 BNM, 2017, Management of Customer Information and Permitted Disclosures, https://www.bnm.gov.my/documents/20124/938039/PD+Management+of+Customer+Info.pdf/0822334e-95b2-0cd9-ecdc-1fbf275a27a2?t=1592247605654%27
231 ZDNet, 2006, Malaysia's new BCM guidelines, https://www.zdnet.com/article/malaysias-new-bcm-guidelines/
232 BNM, 2013, Financial Services Act, https://www.bnm.gov.my/documents/20124///35ed2b4c-1995-f91d-3891-75d69d247d55
233 Daily Host News (2020) Malaysia on the fast lane to become Cloud Computing Hub – Malaysia Cloud & Datacenter Digital Summit 2020, https://www.dailyhostnews.com/malaysia-on-the-fast-lane-to-become-cloud-computing-hub-malaysia-cloud-datacenter-digital-summit-2020#:~:text=The%20Malaysian%20government%20has%20set,impact%20domains%20%E2%80%93%20Governance%20and%20People.
234 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323

Regulatory Recommendations	Malaysia's Scores and Justifications
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.** While explicit approval is only required for material outsourcing, it is for each workload and not each CSP/FI relationship. The Outsourcing Policy Document states that the FI must obtain written approval before a) entering a new material outsourcing arrangement; or (b) making a significant modification to an existing material outsourcing arrangement. All financial institutions must submit an outsourcing plan approved by the Board to BNM within 3 months following the FI's financial year end, including details of all planned outsourcing arrangements, detailed explanation of each outsourcing arrangement, and their overall impact on the FI's staff and talent capacity. The submission of this yearly plan is different from the submission for written approval discussed in the previous paragraph.[235] RMiT document (10.50) states that financial institutions must separately identify critical and non-critical systems, prior to using cloud services. A financial institution must notify the Bank of its intention to use cloud services for non-critical systems. The risk assessment (10.49) must be documented and made available for the Bank's review as and when requested by the Bank. A financial institution is required to consult the Bank prior to the use of the public cloud for critical systems. The risk assessment (10.49) must be conducted, and in addition, the FI must demonstrate other factors such as adequacy of overarching cloud adoption strategy, availability of independent, internationally recognised certifications of cloud service providers, and the degree to which the selected cloud configuration adequately addresses geographical redundancy, high availability, scalability, portability, interoperability, and strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.[236]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**4 points: Yes, to an extent. Regulations clearly differentiate applicability to material and non-material workloads, and non-material workloads are exempt from additional documentary requirements (applicable to material workloads), but other onerous regulatory requirements apply to non-material workloads.** The Outsourcing Policy document defines material outsourcing arrangements and lays out factors in Appendix 3 to assess whether an arrangement is considered material. It specifically mentions that any arrangement involving internal cloud functions (i.e. risk management, internal audit and compliance) would generally be considered as a material outsourcing arrangement. In the same document, regulations are applied to the material and non-material arrangement and there is no differentiation mentioned, other than the written approval requirement discussed in Recommendation 3.[237] In the RMiT document, the FI must **notify** the Bank of its intention to use cloud for non-critical systems and submit a risk assessment. To use cloud for critical systems, it must **consult** with the bank, conduct the risk assessment plus an assessment of additional factors (highlighted in recommendation 3).[238] Therefore, there are less onerous requirements on non-critical outsourcing arrangements.
5. Regulations should have a clear distinction between control vs processing of data	**6 points: Yes, there is a clear distinction between an entity that is a controller versus one that is a processor of data.** According to the PDPA 2010, "data user" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor; "data processor", in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes;[239] RMiT document states that a financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.[240]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** In the Outsourcing Policy The document, it is stated that the FI must ensure where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are comparable to Malaysia.[241] – This is further clarified as: The Bank expects, at the very least, for there to be a national legal or regulatory framework governing data protection (e.g. Malaysia's Personal Data Protection Act 2010) in jurisdictions where a financial institution's data is stored or processed.[242] In the PDPA 2010, it is stated that transfer of personal data to a place outside Malaysia can only be done when such a place has been specified by the Minister, upon the recommendation of the Commissioner, by

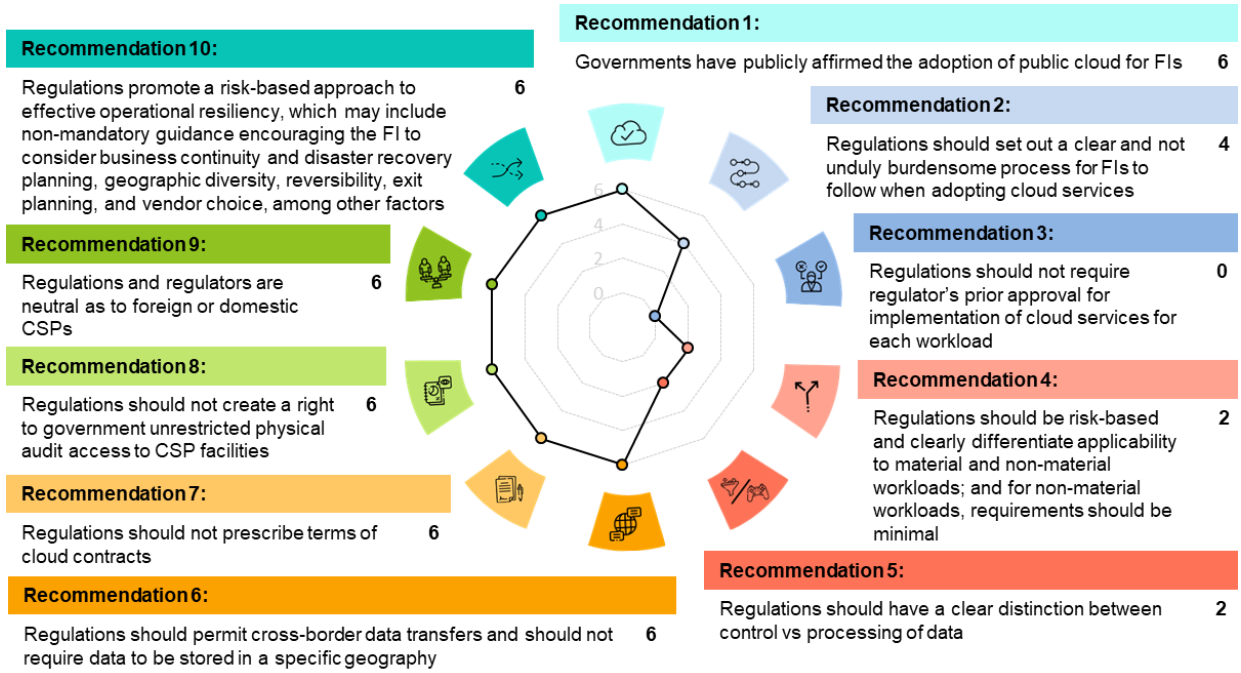
235 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
236 BNM, Jun 2020, Risk Management in Technology (RMiT), https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078
237 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
238 BNM, Jun 2020, Risk Management in Technology (RMiT), https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078
239 Personal Data Protection Act, 2010, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf
240 BNM, Jun 2020, Risk Management in Technology (RMiT), https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078
241 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
242 BNM, 2019, Frequently Asked Questions, Outsourcing, https://www.bnm.gov.my/documents/20124/938039/FAQ_Outsourcing_20191023.pdf/5a53bbfd-86ca-ea21-edc5-af473ee91cc6?t=1592250688407

Regulatory Recommendations	Malaysia's Scores and Justifications
	notification in the Gazette. But this specification has not been made by the Minister. There are exceptions to this, so personal data may be transferred if the individual has given consent, the transfer is necessary for the performance of the contract between the FI and the individual, and the FI has taken all precautions and exercised all due diligence to ensure that the data processing will not in any way contravene the Malaysian PDPA 2010. (Section 129)[243]
b. Regulations should not require data to be stored in a specific geography	**3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** In the PDPA 2010 it is stated that transfer of personal data to a place outside Malaysia can only be done when such a place has been specified by the Minister, upon the recommendation of the Commissioner, by notification in the Gazette. But this specification has not been made by the Minister.
7. Regulations should not prescribe terms of cloud contracts	**2 points: Regulations have overly detailed requirements for the cloud contract, but do not go to the extent of prescribing specific contractual language.** The Outsourcing Policy document highlights what the outsourcing agreement must, at a minimum, provide for. In addition, it mentions that the outsourcing agreement must contain provisions that give the Bank direct access to the systems and information or documents relating to the outsourcing activity, enable the Bank to conduct on-site supervision, enable the Bank to appoint an independent third party to perform a review of the relevant systems, and allow the FI to modify or terminate the arrangement when the Bank issues a direction to it.[244] RMiT document states that FI IT systems are managed by third party service providers, the FI should ensure, including through contract that they provide sufficient notice to the FI before any changes are undertaken that may impact the IT system.[245] These are designated an 'S' in the documents - denotes a standard, an obligation, requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**0 points: Regulations specify that unrestricted physical access is required.** In the Outsourcing Document, the regulations stipulate that the agreement should include provision for the FI and its external auditors to conduct audits and on-site inspections on the service provider and its sub-contractors, and to obtain any report or finding made in relation to the outsourced activity. FI can rely on third-party certifications and reports made available by the cloud service provider, but it is made clear that the FI has the right to conduct on-site inspections where necessary. In addition, it mentions that the outsourcing agreement must contain provisions which give the Bank direct access to the systems and information or documents relating to the outsourcing activity, and enable the Bank to conduct on-site supervision.[246]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** No mention of local office or presence, or any preference treatment for domestic CSPs.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**0 points: Regulations related to operational resiliency do not focus on a risk-based approach to resilience or are prescriptive.** The Outsourcing Policy document states that the FI (specifically the senior management) must develop a risk management framework, and manage outsourcing risks on an institution-wide basis. It additionally states that FI's BCP must consider the possible need for an alternative service provider, including considerations of the limited number of service providers in the market; and the degree of difficulty, cost and time required to integrate the outsourced activity in-house.[247] RMiT document states that FI is required to conduct a comprehensive risk assessment prior to cloud adoption. The assessment must specifically address risks associated with vendor lock-in and application portability or interoperability.[248]

243 Personal Data Protection Act, 2010, http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20709%2014%206%202016.pdf
244 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
245 BNM, Jun 2020, Risk Management in Technology (RMiT), https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078
246 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
247 BNM, Oct 2019, Policy Document on Outsourcing, https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323
248 BNM, Jun 2020, Risk Management in Technology (RMiT), https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078

Philippines

Figure 15: Philippines' Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 44

Market overview and key updates

Bangko Sentral Ng Pilipinas (BSP) is the key regulator of the financial sector in the Philippines. While the BSP regulations acknowledge that cloud technology enhances business flexibility and reduces operational costs, it is the government's Cloud First Policy that has pushed forward cloud adoption in the public and private sectors in the Philippines.

Today, a growing number of FIs are using cloud as BSP allows the necessary flexibility to enter into outsourcing arrangements with CSPs located outside the jurisdiction. However, it does ask FIs to ensure that CSPs are based in jurisdictions that uphold confidentiality and privacy, and continuously monitor political, economic and social risks in those jurisdictions. FIs are however prohibited from outsourcing inherent banking functions such as services related to the placement of deposits and withdrawals, granting of loans, position-taking and market risk-taking activities, managing of risk exposures, and strategic decision-making.

Most recently, BSP has highlighted the importance of data connectivity through a joint statement with the Monetary Authority of Singapore (MAS).[249] The Banks have agreed to allow transfers of data, including personal information across borders, without restricting the location of data storage and processing. Domestically, BSP has pushed for cloud adoption especially in smaller banks and those that serve rural areas, as it is seeing the potential for the cloud in increasing financial inclusion. Last year, Cantilan Bank became the first BSP-regulated rural bank to pioneer cloud-based technology, and others are expected to follow suit.[250] In other initiatives, it has introduced a regulatory sandbox to encourage financial innovation[251]

249 MAS (2020) Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore, https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas
250 Manila Standard, 2019, Cantilan Bank is first BSP regulated Rural Bank to pioneer cloud-based technology, https://www.manilastandard.net/business/287356/cantilan-bank-is-first-bsp-regulated-rural-bank-to-pioneer-cloud-based-technology.html
251 Baker McKenzie, International Guide to Regulatory Fintech Sandboxes, https://www.bakermckenzie.com/en//media/files/insight/publications/2018/12/guide_-intlguideregulatorysandboxes_dec2018.pdf

and a dedicated Financial Technology Subsector (FTSS) to institutionalize the cyber-resilience of the financial system.[252]

Relevant regulator(s)

- Bangko Sentral ng Pilipinas (BSP)[253]
- Department of Information and Communications Technology (DICT)[254]
- National Privacy Commission (NPC)[255]

Relevant regulation(s)

- Enhanced Guidelines on Information Security Management[256]
- Amendments to the Guidelines on Outsourcing[257]
- Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions[258]
- Guidelines On Business Continuity Management[259]
- Technology and Cyber Risk Reporting and Notifications Requirements[260]
- Manual of Regulations for Banks[261]
- Law on Secrecy of Bank Deposits[262]
- Foreign Currency Deposits Act[263]
- General Banking Law of 2000[264]
- Anti-Money Laundering Act of 2001[265]
- Revised Implementing Rules and Regulations of Republic Act No. 9160[266]
- Credit Information System Act[267]
- Data Privacy Act 2012[268]
- Cybercrime Prevention Act of 2012[269]
- Implementing Rules and Regulations of the Cybercrime Prevention Act of 2012[270]

Summary of market alignment with the recommendations

Regulatory Recommendations	Philippines Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**6 points: Yes, public cloud adoption is promoted in a public affirmation.** Circular No 808, Guidelines on Information Technology Risk Management, Appendix 75e acknowledges that the cloud computing model allows BSIs the option to move from a capital-intensive approach to a more flexible business model that lowers operational costs.[271]

252 Business World, 2018, BSP forms fintech unit, https://www.bworldonline.com/bsp-forms-fintech-unit/
253 Bangko Sentral Ng Pilipinas, http://www.bsp.gov.ph/
254 Department of Information and Communications, https://dict.gov.ph/
255 National Privacy Commission, https://www.privacy.gov.ph/
256 BSP, 2017, Circular No. 982, Enhanced Guidelines on Information Security Management , http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c982.pdf
257 BSP, 2016, Circular No. 899, Amendments to the Guidelines on Outsourcing, http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf
258 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
259 BSP, 2017, Circular No. 951, Guidelines On Business Continuity Management , http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c951.pdf
260 BSP, 2018, Circular No. 1019, Technology and Cyber Risk Reporting and Notifications Requirements, http://www.bsp.gov.ph/downloads/regulations/attachments-/2018/c1019.pdf
261 BSP, 2018, Manual of Regulations for Banks, http://www.bsp.gov.ph/downloads/regulations/MORB/2018_MORB.pdf
262 Republic Act No. 1405, Law on Secrecy of Bank Deposits, http://www.pdic.gov.ph/index.php?nid1=10&nid2=3
263 Republic Act No. 6426, Foreign Currency Deposits Act, http://www.bsp.gov.ph/downloads/laws/RA6426.pdf
264 Republic Act No. 8791, General Banking Law of 2000, http://www.bsp.gov.ph/downloads/regulations/gba.pdf
265 Republic Act No. 9160, http://www.bsp.gov.ph/regulations/laws_aml.asp
266 RIRR, 2016, Revised Implementing Rules and Regulations of Republic Act No. 9160, http://www.amlc.gov.ph/laws/money-laundering/2016-revised-implementing-rules-and-regulations-of-republic-act-no-9160-as-amended
267 Republic Act No. 9510, Credit Information System Act, http://www.ctb.com.ph/wp-content/uploads/2010/05/ra-9510-cisa.pdf
268 Republic Act No. 10173, Data Privacy Act 2012, http://www.ctb.com.ph/wp-content/uploads/2010/05/ra-9510-cisa.pdf
269 Republic Act No. 10175, Cybercrime Prevention Act of 2012, https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html
270 Republic Act No. 10175, Implementing Rules and Regulations of the Cybercrime Prevention Act, http://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-actno10175/
271 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf

Regulatory Recommendations	Philippines Scores and Justifications
	Philippines Cloud First Policy – cloud as the preferred technology for government administration and the delivery of government services.[272] Additionally, BSP is encouraging rural banks to adopt cloud, for example, Cantilan Bank has become the first FI regulated by BSP to leverage the cloud. BSP Governor is quoted to have said: "Cloud technology that meets the requirements of the BSP's Circular 808 is enhancing the competitiveness of rural banks and enabling them to provide affordable, high-quality financial services."[273]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.** Circular No 808, Guidelines on Information Technology Risk Management, Appendix 75e, 3, details the steps to be taken before outsourcing, such as risk assessment and due diligence for service provider selection. [274] Circular No 899, Amendments to the Guidelines on Outsourcing also provides details on factors to consider when evaluating and selecting potential service providers; risk assessment for outsourcing activities. [275]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.** Circular No 899, Amendments to the Guidelines on Outsourcing, subsection X162.3: Only those banks with a CAMELS composite rating of at least 3 and a Management rating of not lower than 3 shall be allowed to outsource designated activities *without* prior BSP approval. Otherwise, the bank must secure prior approval from the appropriate department of the SES whose evaluation will be based on the bank's ability to manage risks attendant to outsourcing.[276] Circular No 808, Guidelines on Information Technology Risk Management, Appendix 75e discuss cloud computing model and states BSIs should consult BSP before making any significant commitment on cloud computing.
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**2 points: Differentiation (materiality is defined) is made but same regulations apply to both material and non-material workloads.** Circular No 808, Guidelines on Information Technology Risk Management, Appendix 75e discuss public cloud computing. It is only allowed for non-core operations and business processes (email, office productivity, claims and legal management etc) which do not directly involve sensitive BSI and customer data. Core operations and business processes (Loans, Trust and Treasury systems, ATM switch operations) are not allowed to use public cloud computing. Distinguishing whether a particular actual operation or business is "core" or "non-core" and classifying the data (e.g. confidential, critical, sensitive, public) associated with the system or application are, therefore, significant considerations in determining the permissibility of the public cloud model for this type of operation or process.
5. Regulations should have a clear distinction between control vs processing of data	**2 points: Unclear or ambiguous (e.g. mentions but no definition).** Circular No. 808, Guidelines on Information Technology Risk Management, Annex A: The BSP Supervised Institutions' (BSI's) ownership rights over the data must be firmly established in the contract to enable a basis for trust and privacy of data. Ideally, the contract should state clearly that the organization retains exclusive ownership over its data; that the CSP acquires no rights or licenses through the agreement, to use the BSI's data for its own purposes; and that the CSP does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the CSP. [277] Credit Information System Act, SEC.6 Confidentiality of Credit Information: The Corporation, the outsource entities shall hold the credit information under strict confidentiality and shall use the same only for the declared purpose of establishing the creditworthiness of the borrower. Outsource entities, which may process and consolidate basic credit data, are absolutely prohibited from releasing such data received from the Corporation other than to the Corporation. [278]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** Transfers of data are permitted
b. Regulations should not require data to be stored in a specific geography	**3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** Circular No. 808, Guidelines on Information Technology Risk Management, Annex A: CSP should have some reliable means to ensure that an organization's data is stored and processed only within specific jurisdictions. [279] Circular No 899, Amendments to the Guidelines on Outsourcing: In addition, offshore outsourcing of bank's domestic operations are permitted only when the service provider operates in jurisdictions that uphold confidentiality. When the service provider is located in other countries, the bank should take into account and

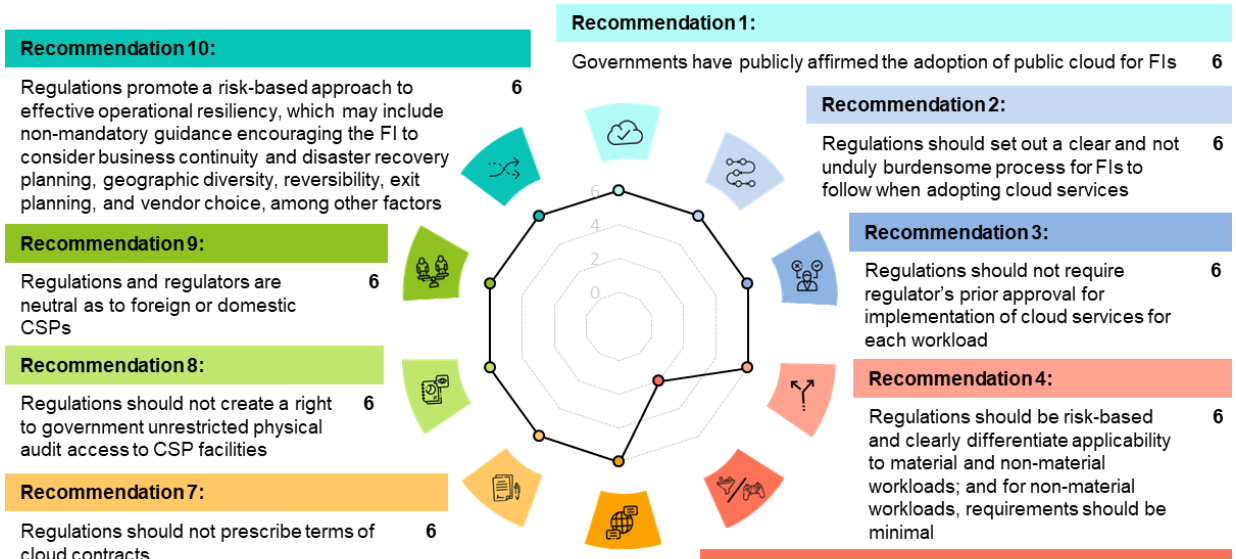
272 DICT, DICT Releases Amended Cloud First Policy for Gov't Transition to "New Normal", https://dict.gov.ph/dict-releases-amended-cloud-first-policy-for-govt-transition-to-new-normal/
273 Manila Standard, 2019, Cantilan Bank is first BSP regulated Rural Bank to pioneer cloud-based technology, https://www.manilastandard.net/business/287356/cantilan-bank-is-first-bsp-regulated-rural-bank-to-pioneer-cloud-based-technology.html
274 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
275 BSP, 2016, Circular No. 899, Amendments to the Guidelines on Outsourcing, http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf
276 BSP, 2016, Circular No. 899, Amendments to the Guidelines on Outsourcing, http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf
277 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
278 Republic Act No. 9510, http://www.ctb.com.ph/wp-content/uploads/2010/05/ra-9510-cisa.pdf
279 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf

Regulatory Recommendations	Philippines Scores and Justifications
	closely monitor, on continuing basis, government policies and other conditions in countries where the service provider is based during risk assessment process.[280]
7. Regulations should not prescribe terms of cloud contracts	**6 points: Regulations are not prescriptive as to terms of a cloud contract.** Circular No 808, Guidelines on Information Technology Risk Management, Appendix 75e, 3.3, provide guidelines on what should be considered and ensured when signing contracts. [281]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no regulatory requirement of a right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports.** Circular No. 808, Guidelines on Information Technology Risk Management, Appendix 75e, Section 5: The BSI should conduct a regular, comprehensive audit of its service provider relationships. The audit scope should include a review of controls and operating procedures that help protect the BSI from losses due to irregularities and willful manipulations. Such responsibility can be assigned to the BSI's IT audit function. In case the BSI has no technical audit expertise, the non-technical audit methods can provide minimum coverage and should be supplemented with comprehensive external IT audits. [282] Circular No. 808, Guidelines on Information Technology Risk Management, Annex A: BSI and the CSP should agree in advance that the former shall have accessibility to the CSP to audit and verify the existence and effectiveness of internal and security controls specified in the SLA. The BSI's audit policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing. It may also be necessary to augment the internal audit staff with additional training and personnel with sufficient expertise in evaluating shared environments and virtualized technologies. In addition, the parties may also agree on the *right to audit clause via external party* as a way to validate other control aspects that are not otherwise accessible or assessable by the BSI's own audit staff. [283]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** No evidence of preferential treatment to domestic CSPs or excessive requirements on foreign CSPs.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** Circular No 808, Guidelines on Information Technology Risk Management, Annex A,[284] Prioritization arrangements in case of multiple/simultaneous disasters; - Retention of onsite and offsite back-up (Whether to maintain an up-to-date backup copy of data at the BSI's premises or stored with a second vendor that has no common points of failure with the CSP); and - Ability to synchronize documents and process data while the client-BSI is offline.[285] Circular No 899, Amendments to the Guidelines on Outsourcing: The contingency plan must indicate whether another service provider will be tapped, or the service/activity will be brought back in-house. It also states that when risk management is deemed inadequate, BSP may direct the bank to terminate, modify, make alternative arrangements or re-integrate the outsourced activity into its operations, as may be necessary. [286]

280 BSP, 2016, Circular No. 899, Amendments to the Guidelines on Outsourcing, http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf
281 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
282 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
283 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
284 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
285 BSP, 2013, Circular No. 808, Guidelines on Information Technology Risk Management for all Banks and Other BSP Supervised Institutions, http://www.bsp.gov.ph-/downloads/regulations/attachments/2013/c808.pdf
286 BSP, 2016, Circular No. 899, Amendments to the Guidelines on Outsourcing, http://www.bsp.gov.ph/downloads/regulations/attachments/2016/c899.pdf

Singapore

Figure 16: Singapore's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 56

Market overview and key updates

The Monetary Authority of Singapore (MAS) is considered one of the most progressive regulators in the world, as it punches above its weight class to be a regulatory decider, rather than a price-taker when it comes to financial policy. Working closely with the industry, in recent years it has established the Singapore Fintech Festival[287] - now an annual affair - as one of the world's major financial innovation events for the industry to gather at, one which COVID-19 has not dampened enthusiasm for.

The MAS has expressed continued support for FIs' use of cloud, evident through recent measures that recognize the importance of cloud in helping FIs weather COVID-19 disruptions. The Digital Acceleration Grant (DAG), for example, was launched in April 2020 to support FIs' and fintech companies' adoption of digital solutions that improve productivity, strengthen operational resilience and risk management and enhance service delivery. Cloud services are listed as one of 11 categories of solutions eligible for the grant.[288]

Other supportive measures include bilateral agreements that seek to ensure that FIs' use of cloud services is not impeded by regulatory restrictions to the cross-border exchange of data. The February 2020 US-Singapore joint statement on Financial Services Data Connectivity, for example, opposes measures that restrict where data can be stored and processed for financial service suppliers.[289] A similar joint statement with the central bank of the Philippines has also been released.[290]

287 Singapore Fintech Festival, https://www.fintechfestival.sg
288 Monetary Authority of Singapore, Digital Acceleration Grant, https://www.mas.gov.sg/development/fintech/digital-acceleration-grant
289 U.S. Department of the Treasury, United States – Singapore Joint Statement on Financial Services Data Connectivity, https://home.treasury.gov/news/press-releases/sm899
290 Monetary Authority of Singapore, Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore, https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas

Further, the MAS has consistently conducted consultation exercises with the industry on outsourcing risk management and technology risk assessments, most notably in 2019 and 2020:

- In February and March 2019, releasing consultation papers on proposed revisions to the Outsourcing guidelines by Banks and Merchant Banks,[291] Technology Risk Management Guidelines,[292] Business Continuity Management Guidelines.[293]
- In December 2020, the MAS also released a consultation on a proposed Notice to Banks and Merchant Banks on Management of Outsourced Relevant Services, which seeks to introduce new requirements for banks and merchant banks to maintain a register of all ongoing outsourced relevant services, with additional requirements (e.g. information protection and outsourcing agreement terms) applying to material ongoing outsourced relevant services.[294]

Other innovations from the MAS since 2017 include:

- In 2018, the MAS also made headlines when it released the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector[295], which was one of the first articulated policies around the use of AI within the FI sector.
- The MAS Financial Sector Technology and Innovation (FSTI) Digital Acceleration Grant (DAG) scheme support Singapore-based smaller financial institutions and FinTech firms adopt digital solutions to improve productivity, strengthen operational resilience, manage risks better, and serve customers better.[296]
- The MAS continues to operate its regulatory sandbox for financial technology, which was first mooted in June 2016[297] as a conducive space for financial firms to test new financial products without running afoul of regulatory and compliance requirements, which may have been a deterrent to product innovation. In Aug 2017, PolicyPal became the first company to graduate from the sandbox with its insurance brokerage service fully-fledged.[298] Further, MAS continued to innovate within its own sandbox, launching in Aug 2019 a Sandbox Express scheme with faster approvals, where pre-defined sandboxes for activities that are low-risk and/or well-understood and easily-contained.[299]
- A related event of note is the establishment of a new international cross-border mediation agreement called the Singapore Convention on Mediation (official name United Nations (UN) Convention on International Settlement Agreements Resulting from Mediation), which was established on 7 August 2020 and will assist businesses in resolving cross-border disputes and further facilitate international trade.[300]

Relevant Regulators

- Monetary Authority of Singapore[301]

---

291 MAS, Consultation Paper on Outsourcing by Banks and Merchant Banks https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-outsourcing-by-banks-and-merchant-banks
292 MAS, Consultation Paper on Proposed Revisions to Technology Risk Management Guidelines, https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-proposed-revisions-to-technology-risk-management-guidelines
293 MAS, Consultation Paper on Proposed Revisions to Business Continuity Management Guidelines, https://www.mas.gov.sg/publications/consultations/2019/-consultation-paper-on-proposed-revisions-to-business-continuity-management-guidelines
294 MAS, Consultation Paper on Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services, https://www.mas.gov.sg/publications/consultations/2020/consultation-paper-on-management-of-outsourced-relevant-services
295 MAS, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT), https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT
296 MAS Financial Sector Technology and Innovation (FSTI) Digital Acceleration Grant (DAG) scheme, https://www.mas.gov.sg/development/fintech/digital-acceleration-grant
297 MAS, Fintech Regulatory Sandbox Guidelines, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-Paper-on-FinTech-Regulatory-Sandbox-Guidelines.pdf
298 OpenGov, November 2017, Updates on Singapore's FinTech Regulatory Sandbox, https://opengovasia.com/updates-on-singapores-fintech-regulatory-sandbox-30-applications-received-first-graduation-in-august-2017/
299 MAS, Media Releases, August 2019, MAS Launches Sandbox Express for Faster Market Testing of Innovative Financial Services, https://www.mas.gov.sg/news/-media-releases/2019/mas-launches-sandbox-express-for-faster-market-testing-of-innovative-financial-services
300 Straits Times, September 2020, Singapore Convention on Mediation comes into force, https://www.straitstimes.com/singapore/singapore-convention-on-mediation-comes-into-force
301 Monetary Authority of Singapore, https://www.mas.gov.sg

- Association of Banks in Singapore[302] - while not a regulator, this industry body holds considerable non-governmental sway within the FI by the weight of its FI representation

Relevant Regulations

- Banking Act[303] and subsidiary legislation the Banking Regulations[304]
- Guidelines on Outsourcing (often called "Outsourcing Guidelines")[305]
- Technology Risk Management Guidelines[306]
- Personal Data Protection Act[307]

Summary of market alignment with the recommendations

Regulatory Recommendations	Singapore's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**6 points: Yes, public cloud adoption is promoted in a public affirmation.** MAS Managing Director Ravi Menon explicitly announced during the Singapore Fintech Festival in 2016 that the MAS has no objections to FIs using the cloud.[308]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**6 points: Yes, regulations set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption (could be through a reference in the regulation itself or in accompanying cloud computing guidelines/ information papers). Such processes are proportionate, practical and not unduly burdensome.** The MAS clearly identifies cloud computing as a service which may be outsourced on its Guidelines on Outsourcing[309] web page, which links to the Guidelines themselves, which itself addresses processes to follow when adopting Cloud Computing in Section 6.
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**6 points: No approval necessary – (compliance with global standards and international third-party certifications are sufficient).** The MAS adopts a risk-based approach towards outsourcing and technology management, both positions which are covered as part of two Guideline documents – the Guidelines on Outsourcing, and the Technology Risk Management Guidelines.[310] Government approval to use cloud computing is not stipulated nor mandated.
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**6 points: Yes, regulations clearly differentiate applicability to material and non-material workloads, and regulations for non-material workloads are light touch (minimal), if any. Criteria for assessing materiality are clearly defined.** Materiality is clearly defined in the Guidelines on Outsourcing,[311] and the MAS expects FIs to address the applicability of regulations insofar as they are commensurate with the nature of risks in, and materiality of the outsourcing arrangement. The applicability of regulations and the level of supervision and oversight to be provided on material workloads are provided throughout the Guidelines on Outsourcing document. In addition, Annex 2 of the Guidelines on Outsourcing specifically addresses how FIs are to differentiate material and non-material workloads.
5. Regulations should have a clear distinction between control vs processing of data	**2 points: Unclear or ambiguous (e.g. mentions but no definition).** The FI's responsibility for its data is specified in the Technology Risk Management Guidelines, in particular Section 3.4 on Management of Third-Party Services, which requires the FI to "assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership".[312] It may be useful to note here that the terms "data controller" and "data processor" are not used in the abovementioned MAS guidelines, nor is it based in the Singapore Personal Data Protection Act 2012 (PDPA)[313]; there is no equivalent for the data controller, although the term "data intermediary" could be construed to be an equivalent term to "data processor". While there is no explicit mention of the control or processing of data, the MAS guidelines are focused on business risk assessment and selecting controls and responsibilities commensurate to the risk levels involved.
6. Geographic Restrictions:	

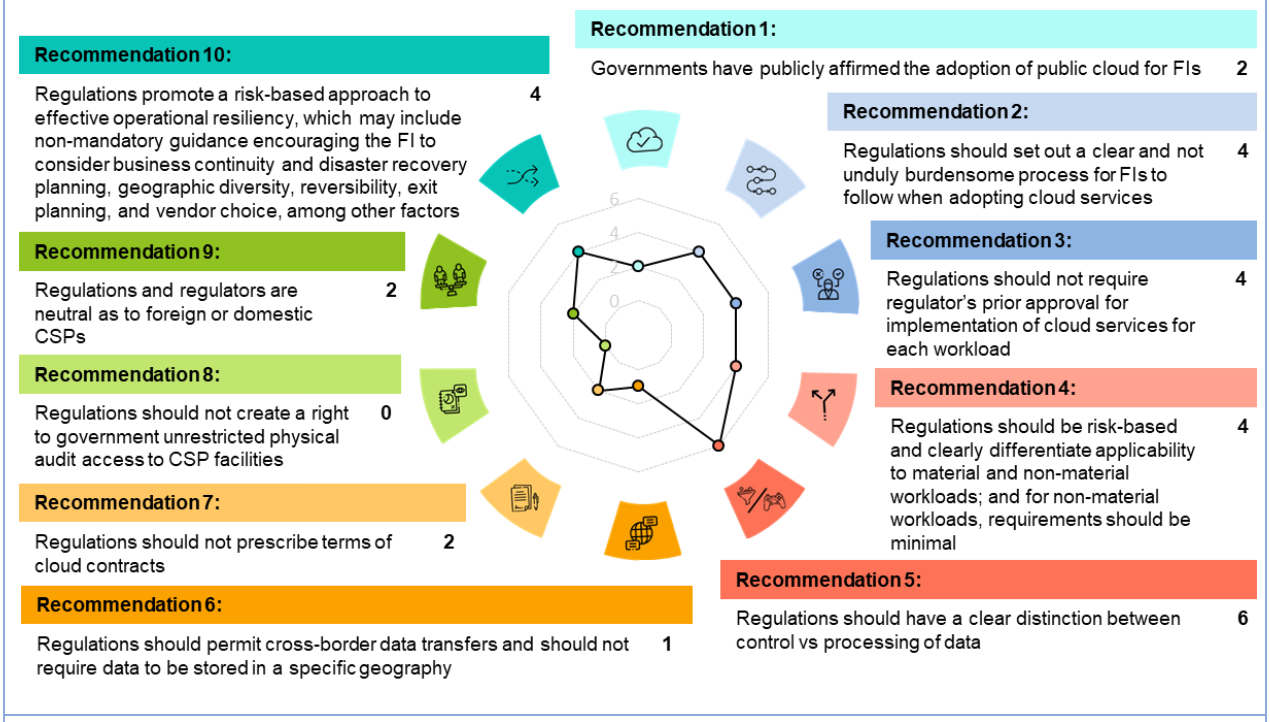
302 The Association of Banks in Singapore, https://www.abs.org.sg
303 Banking Act, 2008, https://sso.agc.gov.sg/Act/BA1970
304 Banking Regulations, 2004, https://sso.agc.gov.sg/SL/BA1970-RG5
305 MAS, Guidelines on Outsourcing, https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing
306 MAS, Technology Risk Management Guidelines, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
307 Personal Data Protection Act, 2012, https://sso.agc.gov.sg/Act/PDPA2012
308 Twitter, Asia Cloud Computing Association, https://twitter.com/accacloud/status/799102882955960320
309 MAS, Guidelines on Outsourcing, https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing
310 MAS, Technology Risk Management Guidelines, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
311 MAS, Guidelines on Outsourcing, https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing
312 MAS, Technology Risk Management Guidelines, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
313 Personal Data Protection Act, 2012, https://sso.agc.gov.sg/Act/PDPA2012

Regulatory Recommendations	Singapore's Scores and Justifications
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** Article 26 of the PDPA specifically addresses the transfer of personal data outside of Singapore, with appropriate exclusions.[314]
b. Regulations should not require data to be stored in a specific geography	**3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** There are no explicit instructions to store data in a particular location as the MAS has taken a risk-management approach towards choice of technology.
7. Regulations should not prescribe terms of cloud contracts	**6 points: Regulations are not prescriptive as to terms of a cloud contract.** The Guidelines on Outsourcing do require contractual arrangements to observe the right of the MAS to exercise its regulatory authority and oversight of the FI, but there are no regulations which prescribe the terms of cloud contracts specifically.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no regulatory requirement of a right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports**. Audits are covered in section 5.9 of the Guidelines on Outsourcing,[315] and clearly state that there may be internal and external auditor reports which may be provided for audit purposes.
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** There are no additional regulatory requirements foreign CSPs need to fulfil in order to provide services to an FI.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** The MAS explicitly calls out the risk-management approach it has taken in section 2.2 of the Technology Risk Management Guidelines,[316] stating that: "The extent and degree to which an FI implements the Guidelines should be commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services." In addition, the Guidelines on Outsourcing require FIs to evaluate and mitigate the risks arising from outsourcing as part of their business continuity management.[317] Section 5.7 states that the FI should take steps to evaluate and satisfy itself that interdependency risks can be adequately mitigated so that the FI can continue to conduct its business with "integrity and competence" in the case of service disruption or failure, or unexpected termination of the outsourcing arrangement, etc. This should involve ensuring that plans and procedures which address such risks to business continuity are put in place, and viable alternatives that allow FIs to resume operations without incurring prohibitive costs are identified.

314 Personal Data Protection Act, 2012, https://sso.agc.gov.sg/Act/PDPA2012
315 MAS, Guidelines on Outsourcing, https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing
316 MAS, Technology Risk Management Guidelines, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
317 The MAS' Business Continuity Management Guidelines provides further guidance on business continuity management practices. MAS, Business Continuity Management Guidelines, https://www.mas.gov.sg/-/media/MAS/resource/legislation_guidelines/securities_futures/sub_legislation/BCMGuidelines.pdf

South Korea

Figure 17: South Korea's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 29

Market overview and key updates

Korea demonstrates the strong growth potential of public cloud. Estimates suggest the cloud market will double in size to USD3billion in 2023.[318] The Financial Services Commission (FSC) sets Korea's financial policies and the Financial Supervisory Service (FSS) enforces them.

From the regulator's perspective, cloud services adoption by FIs is permitted and encouraged. The amendments to the FSC Regulation on Supervision of Electronic Financial Transactions[319] took effect in January 2019 and allow FIs to use cloud services for critical personal information (Unique Personal Information – UPI, and Personal Credit Information – PCI), in addition to non-critical information. However, localization restrictions on critical personal information and detailed reporting requirements may prove to be restrictive. In addition, a recent revision of the Act on Promotion of Information and Communications Network Utilization and Protection now requires global ICT firms with more than 1 million daily users to designate a 'local agent' who can be held responsible in case of data breaches.

Further, the South Korean regulatory landscape is becoming more prescriptive, for example, auditors do not take into account compensatory controls and follow the requirements with precision. The regulatory requirements also change often. These measures may cumulatively serve to slow the growth of the cloud services market in the country. That said, on a positive note, the FSC plans to relax restrictions on cloud services in the financial sector, but no schedule has been detailed as of now.

Overall, the financial services landscape in Korea is highly developed, underpinned by active regulatory and policy initiatives. FSC has undertaken a host of initiatives to promote innovation in the sector, including. In

318 BCG, 2019, Ascent to the Cloud: How Six Key APAC Economies Can Lift-off https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/default
319 FSC, 2018, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_-url=&menu=7210100&no=32676

2019, it set up the sandbox with an initial investment of USD 3.5million. In 2020, it highlighted the success of the sandbox, having raised USD110million in venture capital and launched 36 fintech services.[320] It also formally launched the open banking service in 2019 to allow customers to use a single mobile application to access accounts at different FIs.[321]

Relevant regulator(s)

- Financial Services Commission (FSC)[322]
- Financial Supervisory Service (FSS)[323]
- Personal Information Protection Commission (PIPC)[324]
- Korea Communications Commission (KCC)[325]

Relevant regulation(s)

- Regulation on Supervision of Electronic Financial Transactions, Sept 2018[326]
- The Act on the Development of Cloud Computing and Protection of Its Users[327]
- The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.[328]
- Partial amendment of the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.[329]
- Banking Act (as at 2017)[330]
- Regulation on Business Delegation of Financial Institutions[331]
- Regulations on Consignment of information processing business of financial companies[332]
- The Personal Information Protection Act (PIPA) as amended in 2020[333]
- FSI Guidelines on Use of Cloud Services in the Financial Industry[334]
- Credit Information Use and Protection Act[335]

320 Fintech Futures, 2020, South Korea's fintech sandbox lands $110m and creates 380 jobs, https://www.fintechfutures.com/2020/05/south-koreas-fintech-sandbox-lands-110m-and-creates-380-jobs/
321 Korea Bizwire, 2019, S. Korea Formally Launches Open Banking Service, http://koreabizwire.com/s-korea-formally-launches-open-banking-service/149763
322 Financial Services Commission, http://meng.fsc.go.kr/
323 Financial Supervisory Service, http://english.fss.or.kr/fss/eng/main.jsp
324 Personal Information Protection Commission, https://www.ppc.go.jp/en/
325 Korea Communications Commission, https://eng.kcc.go.kr
326 FSC, 2018, Regulation on Supervision of Electronic Financial Transactions, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_-url=&menu=7210100&no=32676
327 Act on the Development of Cloud Computing and Protection of its Users, 2015, https://elaw.klri.re.kr/eng_mobile/viewer.do?-hseq=35630&type=part&key=43
328 KCC, 2018, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=50484&lang=ENG
329 KCC, 2020, https://opinion.lawmaking.go.kr/gcom/ogLmPp/59972?opYn=-Y&cptOfiOrgCd=1570100&isOgYn=Y&edYdFmt=2020.+8.+24.&stYdFmt=2020.+2.+1.&btnType=1
330 Banking Act, 2017, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=43323&lang=ENG
331 FSS, Regulation on Business Delegation of Financial Institutions, https://english.fss.or.kr/fss/eng/wpge/eng340_viewer.jsp?FileName=R16
332 FSC, Regulations on Consignment of information processing business of financial companies, https://www.law.go.kr/LSW/admRulLsInfoP.do?vSct=%EA%B8%88%EC%9C%B5%ED%9A%8C%EC%82-%AC%EC%9D%98+%EC%A0%95%EB%B3%B4%EC%B2%98%EB%A6%AC&admRulSeq=2100000022989
333 Personal Information Protection Act, 2020, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
334 FSEC, https://www.fsec.or.kr/user/bbs/fsec/41/18/bbsData-View/508.do?page=5&column=&search=&searchS-Date=&searchEDate=&bbsDataCategory
335 FSC, Credit Information Use and Protection Act, http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=46276&type=part&key-=23

Summary of market alignment with the recommendations

Regulatory Recommendations	South Korea's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**2 points: Cloud benefits generally acknowledged, no mention of public cloud.** To promote and develop cloud computing services, Korea has adopted the Act on the Development of Cloud Computing and Protection of its Users (the Cloud Computing Act).[336]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed.** In the amendments to the Regulation on Supervision of Electronic Financial Transactions, when using cloud, the FI must report to the regulator on the measures to provide security and the contents of the contract (provided that non-critical information is also requested by the regulatory authorities).[337]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**4 points: Regulations do not require regulator's prior approval (formal or de facto) for non-material workloads. For material workloads, a regulator's approval (formal or de facto) is required, but it is not required for each workload.** Regulations do not require the FI to obtain the regulator's approval for each material workload moved to a CSP. Although a 'notice' regime, the notification process is burdensome and results in a 'de facto' approval.[338]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**4 points: Yes, to an extent. Regulations clearly differentiate applicability to material and non-material workloads, and non-material workloads are exempt from additional documentary requirements (applicable to material workloads), but other regulatory requirements apply to non-material workloads.** In the 2016 amendment to the Regulation on Supervision of Electronic Financial Transactions, a distinction was made, allowing only non-critical workloads to be available on the cloud. In the 2018 Amendment to Regulation on Supervision of Electronic Financial Transactions, critical or material workloads (personal credit information and unique identification information) were also allowed on the cloud.[339] Reporting requirements exist for both non-critical and critical workloads. Based on the Regulations on Consignment of Information Processing business of financial companies, an outsourcing report must be made when using cloud for non-critical workloads.[340] The Regulation on Supervision of Electronic Financial Transactions, however, states that detailed report with due diligence, business continuity or security measures are to be given prior to using the cloud, for significant workloads only.
5. Regulations should have a clear distinction between control vs processing of data	**6 points: Yes, there is a clear distinction between an entity that is a controller versus one that is a processor of data.** As per PIPA, personal information controller is defined. It means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities; Article 26 of PIPA details outsourcing of personal information processing to an 'outsourcee' by personal information controller, the 'outsourcer'.[341]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**1 points: Not allowed, with some exceptions.** FIs are subject to data localization requirements. The 2018 Amendment to the Electronic Financial Supervisory Regulations (effective from 1/1/19) mandates that FIs only process 'unique personal information' and 'personal credit information' in KR. However, non-critical personal information can be processed overseas, subject to the safeguards provided for in the PIPA and other personal information protection regulations.[342]
b. Regulations should not require data to be stored in a specific geography	**0 points: Data must be stored in specific geographic locations.** FI must store customers critical information within the country.
7. Regulations should not prescribe terms of cloud contracts	**2 points: Regulations have overly-detailed requirements for the cloud contract, but do not go to the extent of prescribing specific contractual language.** Regulation on Business Delegation of FI, Appendix 2 mentions the main provisions of a business delegation agreement. These include the scope of delegated business, method of performance of a delegated business, powers of audit, fees and considerations for business delegation, matters relating to the protection of customers information and confidentiality, emergency plans, provisions for cancellation of the agreement, obligation to accept the investigation by the regulatory authority, cases of sub-delegation and other necessary matters for risk management. It is added that FI may add or subtract from the above matters, taking into account the financial business areas it engages in and characteristics of the counter party.[343]

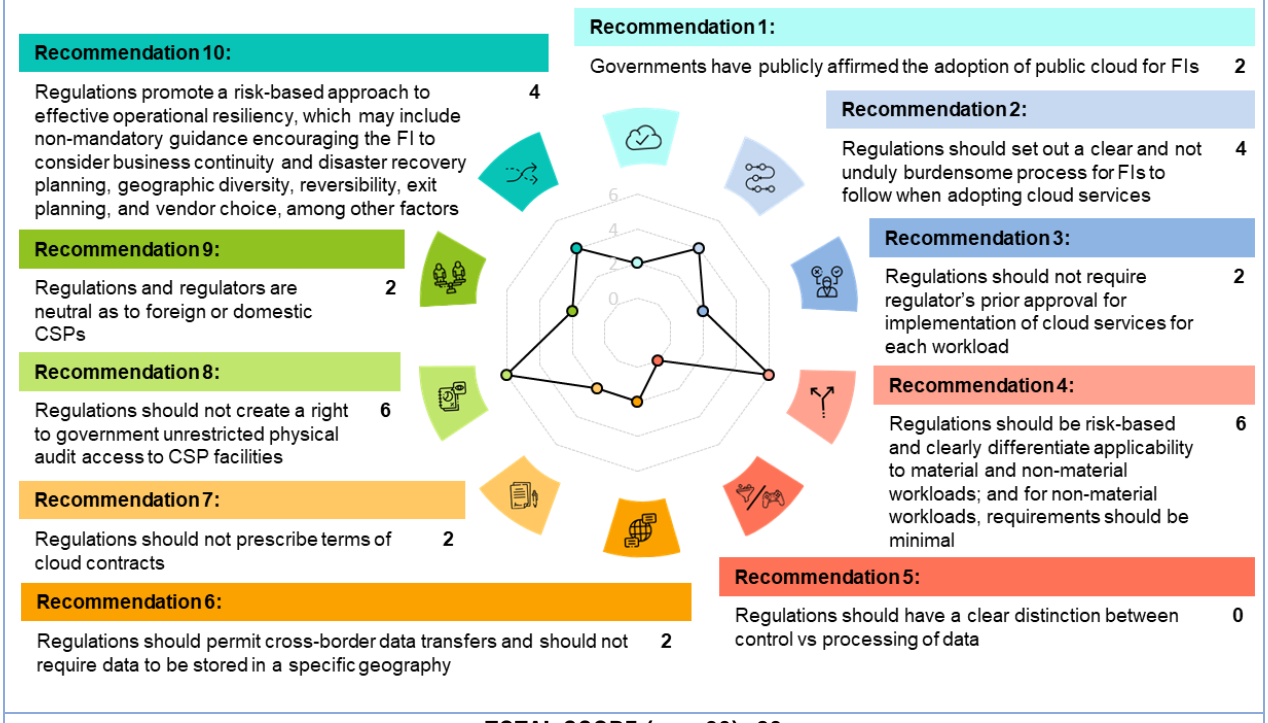
336 Act on the Development of Cloud Computing and Protection of its Users, 2015, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=35630&type=part&key=43
337 FSC, 2018, Regulation on Supervision of Electronic Financial Transactions, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_url=&menu=72-10100&no=32676
338 FSC Regulations on Consignment of information processing business of financial companies, https://www.law.go.kr/LSW/admRulLsInfoP.do?vSct=%EA%B8%88%EC%9C%B5%ED%9A%8C%EC%82%AC%EC-%9D%98+%EC%A0%95%EB%B3%B4%EC%B2%98%EB%A6%AC&admRulSeq=2100000022989
339 FSC, 2018, Regulation on Supervision of Electronic Financial Transactions, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_url=&menu=72-10100&no=32676
340 FSC, Regulations on Consignment of information processing business of financial companies, https://www.law.go.kr/LSW/admRulLsInfoP.do?vSct=%EA%B8%88%EC%9C%B5%ED%9A%8C%EC%82%AC%EC-%9D%98+%EC%A0%95%EB%B3%B4%EC%B2%98%EB%A6%AC&admRulSeq=2100000022989
341 Personal Information Protection Act, 2020, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
342 FSC, 2018, Regulation on Supervision of Electronic Financial Transactions, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_url=&menu=7210100&no=32676
343 FSS, Regulation on Business Delegation of Financial Institutions, https://english.fss.or.kr/fss/eng/wpge/eng340_viewer.jsp?FileName=R16

Regulatory Recommendations	South Korea's Scores and Justifications
	2018 Amendment to the Regulation on Supervision of Electronic Financial Transactions requires that the rights of regulators to monitor and investigate CSPs be specified in cloud contracts, and obligates FIs to report the contents of such contracts to the relevant authorities.[344]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**0 points: Regulations specify that unrestricted physical access is required.** Regulations give the regulator physical access. FSS can audit and inspect FIs and CSPs, and Ministry of Science and ICT can also audit a CSP in case of any violation under the Cloud Act. 2018 Amendment to the Regulation on Supervision of Electronic Financial Transactions requires FIs and CSPs to give the audit right to the regulator via the cloud contract between FIs and CSPs.[345]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**2 points: Some clear distinction in regulations for domestic CSPs disadvantaging foreign CSPs (e.g. requires local address, local representative office).** A revision of the Act on Promotion of Information and Communications Network Utilization and Protection took effect in March 2019 and requires global ICT firms with more than one million daily users or annual sales exceeding USD 900 million to designate a "local agent" who can be held responsible in case of a data breach or other consumer protection violation. A revision to the Value-Added Tax Act passed in December 2018 and taking effect in July 2019 orders the National Tax Service to apply the standard 10 percent VAT tax on revenue earned in the ROK by foreign ICT firms. [346]
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**4 points: Regulations promote a risk-based approach to operational resiliency and are not prescriptive, but do not include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.** No mention of multiple cloud, alternate service providers, interoperability, or reversibility. There is mention of exit strategies. Regulation on Business Delegation of FI, Appendix 2 mentions the main provisions of a business delegation agreement. This includes provisions for cancellation or termination of the business delegation agreement (such as right of termination of the delegator, restoration of information, etc). Other matters necessary for risk management according to the business delegation must also be considered.[347]

344 FSC, 2018, Regulation on Supervision of Electronic Financial Transactions, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_-url=&menu=7210100&no=32676
345 FSC, 2018, Regulation on Supervision of Electronic Financial Transactions, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=3&sch1=&sword=&r_-url=&menu=7210100&no=32676
346 Doing Business in Korea: 2019 Country Commercial Guide for U.S Companies, https://2016.export.gov/southkorea/build/groups/public/@eg_kr/documents/-webcontent/eg_kr_129237.pdf
347 FSS, Regulation on Business Delegation of Financial Institutions, https://english.fss.or.kr/fss/eng/wpge/eng340_viewer.jsp?FileName=R16

Taiwan

Figure 18: Taiwan's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 30

Market overview and key updates

Taiwan government's policy supports fintech innovation, core technologies and applications development have continued to drive R&D and infrastructure investment from multinational companies. For instance, Google is committed to establishing its third data center facility in Taiwan after the company announced its plan to build a second one in Tainan last year, making Taiwan its largest data center hub in Asia Pacific.[348]

FSC's support of the adoption of cloud-based services and technologies by FIs is evident in the amendments of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation effective in September 2019. Article 19-1 and Article 19-2 are specifically introduced to provide guidance on the outsourcing of operations that involve cloud-based services on the understanding that cloud services can benefit financial institutions through operational efficiency improvements and cost reduction. [349]

The regulator aimed to strike a balance between strengthening customer protection and enhancing the service quality of financial institutions. While the regulations clearly distinguish between outsourcing of material operations and non-material operations where the requirements of the latter are simplified, pre-approval from FSC is mandated for outsourcing operations to a CSP in a foreign jurisdiction and it is required that the data protection regulations in the location for data processing and storage must be no less stringent than the regulations in Taiwan.[350]

348 Taiwan News, 2020, Google confirms plans to build 3rd data center in Taiwan, https://www.taiwannews.com.tw/en/news/4001183
349 Financial Supervisory Commission (2019) Press release on Amendments to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=201910220020&aplistdn=ou=news,ou=multisite,ou=english,ou=ap_root,o=fsc,c=tw&dtable=News
350 Financial Supervisory Commission (2019) Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380200

Other major initiatives to foster the development of the financial sector include:

- The passing of the Financial Technology Development and Innovative Experimentation Act[351] and related implementation regulations by the Legislative Yuan on 31 Jan 2018 to promote the development of innovative technologies for the finance industry, through the adoption of the regulatory sandbox.
- With the establishing of FinTech Space[352] in September 2018, a co-working space funded by the government for fintech startups, FSC has facilitated ongoing interactions and communications between the financial and technology sectors and attracted global talents.
- The Standards Governing the Establishment of Commercial Banks have been revised in November 2018[353] to allow the establishment of virtual banks to further enhance competition. In August 2019, FSC awarded three digital banking operating licences to LINE Bank, Next Bank and Rakuten Bank.
- FSC unveiled an Information Security Action Plan for the financial services industry in August to guide the FIs to review their information security strategies, technologies and management systems to ensure secure, convenient and uninterrupted financial services.[354]

Relevant regulator(s)

- Financial Supervisory Commission (FSC)[355]
- Central Bank of the Republic of China[356]
- National Development Council (NDC)[357]

Relevant regulation(s)

- Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation[358]
- Personal Data Protection Act (PDPA)[359]
- Cyber Security Management Act[360]
- Regulations Governing the Security Maintenance and Administration of Financial Institutions[361]
- Consumer Protection Act[362]

351311 Financial Supervisory Commission (2018) Financial Technology Development and Innovative Experimentation Act, https://law.fsc.gov.tw/law/EngLawContent.aspx?lan=E&id=2104&KW=%e9%87%91%e8%9e%8d%e7%a7%91%e6%8a%80
352 FinTechSpace, https://www.fintechspace.com.tw/en/about-us/
353 Financial Supervisory Commission (2018) FSC announced related regulations regarding internet-only banks establishment and started to accept applications, https://www.fsc.gov.tw/en/home.jsp?id=74&parentpath=0,2&mcustomize=multimessage_view.jsp&aplistdn=ou=Bulletin,ou=multisite,ou=english,ou=ap_root,o=fsc,c=tw&dataserno=201812070001&dtable=Bulletin
354 Financial Supervisory Commission (2020) Important Measures, https://www.fsc.gov.tw/en/home.jsp?id=74&parentpath=0&mcustomize=multimessage_view.jsp&dataserno=202009090001&aplistdn=ou=bulletin,ou-=multisite,ou=english,ou=ap_root,o=fsc,c=tw&dtable=Bulletin
355 Financial Supervisory Commission, https://www.fsc.gov.tw/en/
356 Central Bank of the Republic of China, https://www.cbc.gov.tw/en/mp-2.html
357 National Development Council, https://www.ndc.gov.tw/en/
358 Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://law.moj.gov.tw/ENG/LawClass/-LawAll.aspx?pcode=G0380200
359 Personal Data Protection Act, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021#:~:text=The%20Personal%20Data%20Protection%20Act,proper%20use%20of%20personal%20data.&text=%22data%20subject%22%20refers%20to%20an,is%20collected%2C%20processed%20or%20used.
360 Cyber Security Management Act, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297
361 Regulations Governing the Security Maintenance and Administration of Financial Institutions, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380196
362 Consumer Protection Act, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0170001

Summary of market alignment with the recommendations

Regulatory Recommendations	Taiwan's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**2 points: Cloud benefits generally acknowledged, no mention of public cloud.** FSC amended the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation in 2019 to facilitate the use of cloud service.[363]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.** Regulations have set out a clear process that applies explicitly to cloud-based services. However, when the outsourcing operations are material or the operations are outsourced to overseas service providers, FIs are required to submit a number of documents to the competent authority for application and approval before outsourcing, which is relatively burdensome.
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**2 points: Regulations require prior approval (or notice to the regulator and a letter of non-objection) for each CSP/Bank relationship and not each workload, but do not have the clarity of process described for 4 points. The approval process is not clearly described, or does not follow a transparent and objective process with clear requirements, prompt deadlines and criteria for approval and offer the FI or CSP a right to appeal.** Article 18 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation requires financial institutions to submit various documents to the competent authority for approval when outsourcing its operations to overseas service providers and Article 19-2 further states that when outsourced operations involve cloud-based services, and outsourcing operations are material, financial institutions are required to submit additional documents to the competent authority for approval before outsourcing.[364]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**6 points: Yes, regulations clearly differentiate applicability to material and non-material workloads, and regulations for non-material workloads are light touch (minimal), if any. Criteria for assessing materiality are clearly defined.** Under Article 19-2 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, material operations are defined as meeting one of the following conditions: 1. Where outsourced operations cannot be performed or where there are concerns for information security, and such issues have a significant impact on businesses performed by the financial institution. 2. Where an incident on customer data security occurs in the outsourced operations and such incident has a significant impact on the rights and interests of the financial institution or customers. 3. Other issues having significant impact on the rights and interests of the financial institution or customers. When outsourcing operations are material, financial institutions shall submit various documents to the competent authority for approval before outsourcing. Where the financial institution outsources operations involving cloud-based services that are not material outsourcing or where it does not outsource operations to a foreign country in accordance with Article 18, it shall submit the documents specified in Paragraph 1, Subparagraph 3 to Subparagraph 5 to the competent authority for reference.[365]
5. Regulations should have a clear distinction between control vs processing of data	**0 point: No differentiation and all workloads are treated equally.** The Personal Data Protection Act (PDPA) does not adopt any specific term to refer to a party that is performing the function of a data controller as defined under the GDPR. The PDPA applies to all government agencies and non-government agencies that are collecting, processing, and using personal data. Under PDPA, the term 'data processor' does not exist. A similar concept would be the commissioned agency that has been appointed by a government agency or a non-government agency to collect, process, or use personal data for and on behalf of such a government agency or non-government agency. [366]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**1 point: Not allowed, with some exceptions.** According to Article 19-1 Paragraph 7 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, where customer data is outsourced to a cloud service provider, the location for processing and storage shall be within the territories of the R.O.C. in principle. The regulations do not elaborate on what in principle means but stating that if the data are located outside the territories, the following rules shall apply:

363 Financial Supervisory Commission (2019) Press release on Amendments to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno-=201910220020&aplistdn=ou=news,ou=multisite,ou=english,ou=ap_root,o=fsc,c=tw&dtable=News

364 Financial Supervisory Commission (2019 Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380200

365 Financial Supervisory Commission (2019 Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380200

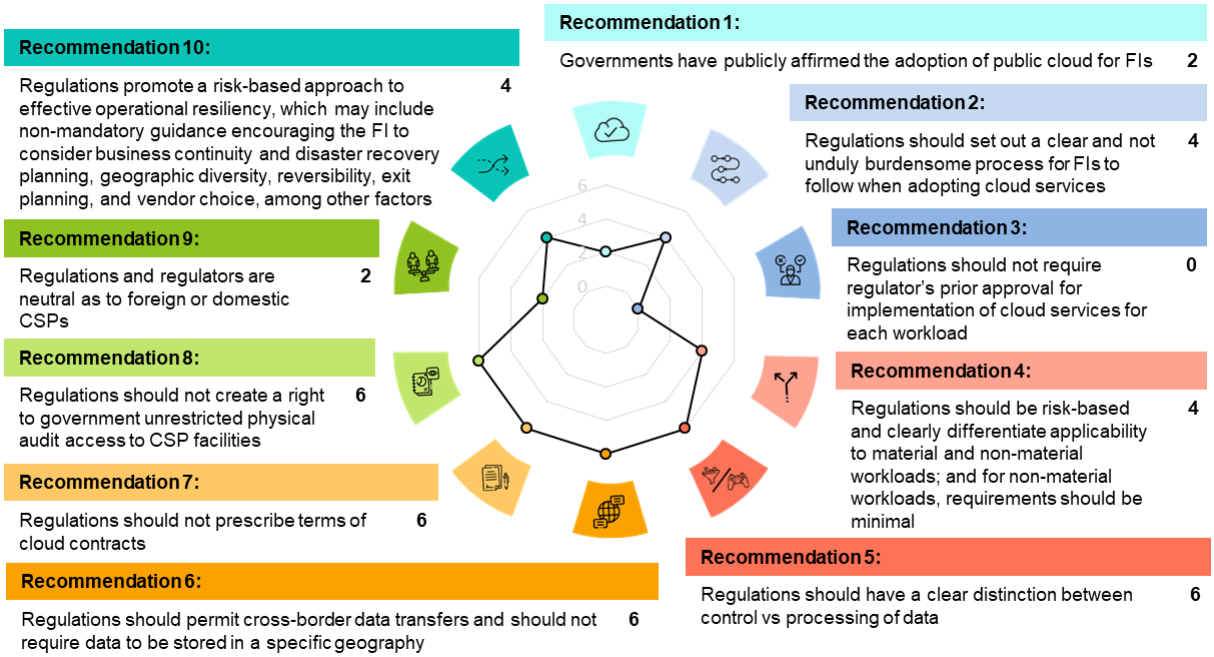
366 National Development Council (2015) Personal Data Protection Act (PDPA), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021#:~:text=The%20Personal%20Data%20Protection%20Act,proper%20use%20of%20personal%20data.&text=%22data%20subject%22%20refers%20to%20an,is%20collected%2C%20processed%20or%20used

Regulatory Recommendations	Taiwan's Scores and Justifications
	(1) The financial institution shall retain rights to designate the location for the processing and storage of the data. (2) The local data protection regulations in above location shall not be lower than the requirements of the R.O.C. (3) Except with the approval of the competent authority, backups of customer important data shall be retained in the R.O.C. On the contrary, cross-border transfer of personal data is permitted in principle under Article 21 of the PDPA unless the competent authorities have issued any orders to prohibit the transfer. [367]
b. Regulations should not require data to be stored in a specific geography	**1 point: No, only 'white listed' jurisdictions allowed.** As explained above in 6a
7. Regulations should not prescribe terms of cloud contracts	**2 points: Regulations have overly-detailed requirements for the cloud contract, but do not go to the extent of prescribing specific contractual language.** Article 10 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation prescribes key terms of an outsourcing agreement including the responsibilities of service providers, customer protection and risk management obligations, allowing regulators the right to access relevant data or reports and conduct a financial examination. Also, system recovery requirements are prescribed for banks as they shall assure the functional operations of deposit, withdrawal and payment transactions of existing customers within four hours after the offshore information system fails to provide services, The bank shall ensure the functional operations of its credit and other major businesses in Taiwan within seven days of the incident, through activation of the backup system, installation of (temporary) information server or other means, provided it is evaluated that the offshore information system could not be functional within a short period of time due to a natural disaster.(Article 18)[368]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no regulatory requirement of a right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports.** The Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation do not require unrestricted audit access rights to financial institutions. The financial institution shall ensure that the competent authority, the Central Bank, or their designated representatives have access to related information on the outsourced operations executed by cloud service providers, including the audit report of customer information relevant systems, and on-site audit rights. The competent authority and the Central Bank may access relevant data or reports and conduct related financial examinations on the outsourced operations of a financial institution. Financial institutions shall conduct at least one routine audit and one target audit annually. They may appoint an independent third party with expertise in information technology at its sole discretion or in conjunction with other financial institutions that outsource to the same cloud service provider to conduct the audits.[369]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**2 points: Some clear distinction in regulations for domestic CSPs disadvantaging foreign CSPs (e.g. requires local address, local representative office).** There is clear distinction in the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation between domestic CSPs and foreign CSPs. When operations are outsourced to overseas service providers, FIs need to submit various documents to the competent authority for application and approval.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**4 points: Regulations promote a risk-based approach to operational resiliency and are not prescriptive, but do not include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.** Although the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation emphasize that financial institutions shall ensure proper control of operational risks and fully evaluate the risks of cloud service providers, it does not provide guidance to encourage geographic diversity and vendor choice and consider disaster recovery planning.

367 National Development Council (2015) Personal Data Protection Act (PDPA), https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021#:~:text=The%20Personal%20Data%20Protection%20Act,proper%20use%20of%20personal%20data.&text=%22data%20subject%22%20refers%20to%20an,is%20collected%2C%20processed%20or%20used.
368 Financial Supervisory Commission (2019 Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380200
369 Financial Supervisory Commission (2019 Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380200

Thailand

Figure 19: Thailand's Implementation of Regulatory Recommendations



TOTAL SCORE (max 60): 40

Market overview and key updates

Thailand has a thriving financial services landscape, and the government is supporting digital transformation in the sector through key policy initiatives. These include the launch of fintech regulatory sandbox in 2017, the introduction of a National e-Payment Master Plan, and PromptPay, a real-time payments system to advance digital payments, and the Bangkok Fintech Fair in 2018.[370]

FIs in Thailand are gradually adopting cloud, with the Bank of Thailand (BoT) both permitting and supporting this transition. In recent years BoT regulations have strived to simplify processes and reduce regulatory requirements on FIs trying to outsource.[371] It encourages FIs to group work functions to outsource.

BOT has recently updated its regulatory framework such that financial institutions are responsible for self-classifying the significance of their workloads. Commercial banks and payment service business providers are then required to notify BOT at least 15 days in advance before deploying or changing existing systems that they self-classify as "significant". Finance companies and credit fonciers must seek prior approval from BOT before deploying of changing "significant."[372]

However, several laws and regulations have been introduced, including the Electronic Transaction Act[373], Personal Data Protection Act[374] and Cybersecurity Act[375]. These will serve to enhance the legal infrastructure around trusted and secure transfers of data, supporting the digitalization and cloud adoption by FIs.

370 BOT, 2019, Payment Systems Roadmap, https://www.bot.or.th/English/PaymentSystems/PolicyPS/Documents/PaymentRoadmap_2021.pdf
371 BOT, 8-2557, Regulations on Outsourcing of Financial Institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2558/EngPDF/25580002.pdf
372 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
373 SilkLegal, 2019, Thailand Facilitates Key Digital Reforms Through Electronic Transaction Act Amendments, https://silklegal.com/thailand-facilitates/
374 Government Gazette, 2019, https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf
375 Government Gazette, 2019, https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf

Relevant regulator(s)

- Bank of Thailand (BOT)[376]
- Office of the Personal Data Protection Committee (PDPC)
- Electronic Transactions Development Agency (ETDA)[377]

Relevant regulation(s)

- Cybersecurity Act[378]
- Personal Data Protection Act[379]
- Regulations on supervision of information technology risks of financial institutions, BOT SorNorSor. 21/2562 (unofficial translation) [380]
- Announcement of the Electronic Transactions Commission On Cloud Service Usage Guidelines[381] (unofficial translation)

Summary of market alignment with the recommendations

Regulatory Recommendations	Thailand's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**2 points: Cloud benefits generally acknowledged, no mention of public cloud.** No government affirmation of public cloud.
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**4 points: Yes, regulations set out a clear process for FIs to follow when entering into outsourcing arrangements in general but applicability to cloud is not explicitly addressed, and/or processes are relatively burdensome.** Regulation on Outsourcing of FI detail the process for applying for permission to outsource, cases in which permission or approval are needed is very clear.[382] The Regulations on Supervision of IT Risks, 8, mentions detailed factors to consider for selection of service provider, including what should be included in due diligence.[383]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**0 points: Regulations require the FI to obtain the regulator's approval for each workload moved to a CSP.** Financial institutions to self-classify the significance of their workloads. Commercial banks and payment service business providers are required to notify BOT at least 15 days in advance before deploying or changing existing systems that they self-classify as "significant". Finance companies and credit financiers must seek prior approval from BOT before deploying of changing "significant." [384]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**4 points: Yes, to an extent.** BOT allows financial institutions to self-classify "significant" workloads based on its internal criteria mutually agreed by the first and second lines of defenses and designated internal oversight committees. The criteria must consider the risk and impact on business operations of the financial institution on a wide scale (bank wide impact), such as where the majority of customers may be affected, and impact on the financial institution system (banking system wide impact), such as where the shared service infrastructure of the financial institution system may be affected.[385]
5. Regulations should have a clear distinction between control vs processing of data	**6 points: Yes, there is a clear distinction between an entity that is a controller versus one that is a processor of data.** The PDPA makes a distinction between data controller and data processor. The data controller has the duty to keep the personal data secure, through appropriate security measures, and preventing the data processor from using or disclosing such personal data unlawfully.[386]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** Under the PDPA one of three conditions for international transfers:

376 Bank of Thailand, https://www.bot.or.th/English/Pages/default.aspx
377 Electronic Transactions Development Agency, https://www.etda.or.th/
378 Government Gazette, 2019, https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf
379 Government Gazette, 2019, https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf
380 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
381 Government Gazette, 2019, http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/E/149/T_0039.PDF
382 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
383 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
384 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
385 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
386 Thailand Personal Data Protection Law, https://www.dataprotectionreport.com/2020/02/thailand-personal-data-protection-law/

Regulatory Recommendations	Thailand's Scores and Justifications
	• Transfer to a country that has established strong data protection measures that comply with the guidelines defined by the Personal Data Protection Committee; • Consent; and • A pre-existing contract between the data owner and the controller. • the transfer is in the interest of the data subject who is incapable of giving consent The guideline on adequate data protection standard is yet to be issued.[387]
b. Regulations should not require data to be stored in a specific geography	**3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** The PDPA states that the personal data must not be transferred to third countries which do not provide adequate protection.
7. Regulations should not prescribe terms of cloud contracts	**6 points: Regulations are not prescriptive as to terms of a cloud contract.** A financial institution must specify details and conditions in a service contract or service level agreement with third-party providers, according to the risk level and materiality of the use of service, connection of systems and data access. These include scope of the use of third-party service, roles and responsibilities of the cloud service provider and financial institution, minimum operating standards, ongoing monitoring of third-party provider's performance, etc.[388]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no regulatory requirement of a right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports.** A financial institution should arrange for the Bank of Thailand, internal auditors or external auditors appointed by the financial institution to examine third-party providers for "parts" related to the use of service provided by connection of systems to and data access by such third-party providers, specified in a service contract or service level agreement. A financial institution may also use the results of IT examination of the third-party provider certified by external auditors that meet internationally accepted standards, such as SSAE 18 (SOC 2 Type 2 Report) or PCI-DSS Attestation of Compliance (AOC) and are endorsed by the board of directors or designated senior executives.[389]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**2 points: Some clear distinction in regulations for domestic CSPs disadvantaging foreign CSPs (e.g. requires local address, local representative office).** Government policies may encourage domestic procurement and end up given preferential treatment to domestic CSPs. For instance, for public sector purchases, the 1992 Prime Minister's Office Regulation on Procurement (as amended) provides a preference for domestic goods and services by using a range of initiatives such as price preference margin for all local suppliers, the requirement of having a Thai leading firm for services contracts or 50% engagement of Thai personnel to be engaged on the project.[390]
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**4 points: Regulations promote a risk-based approach to operational resiliency and are not prescriptive, but do not include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors.** The Regulations on Supervision of IT Risks state that FI must set clear and appropriate criteria in the selection of third parties to provide services, such as the reliability of the system and the service providers that they are certified under international standards or relevant IT standards. The flexibility to change the service provider must be considered, due to technology change or changes in business strategy.[391] The Cloud Service Usage Guidelines state that the contract should define a course of action, such as the period for access to the user's information and service provider's data retention period, and determining the service termination plan (exit plan).[392]

387 Focal Point, 2019, Data Protection in Thailand: A Summary of the PDPA, https://blog.focal-point.com/data-protection-in-thailand-what-you-need-to-know-about-thepdpa
388 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
389 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
390 BSA, 2018, Thailand Country Report, https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_-Report_Thailand.pdf
391 BOT, 2019, SorNorSor. 21/2562, Regulations on supervision of information technology risks of financial institutions, https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620272.pdf
392 Government Gazette, 2019, http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/E/149/T_0039.PDF

United Kingdom (UK)

Figure 20: United Kingdom's Implementation of Regulatory Recommendations

Recommendation 1:
Governments have publicly affirmed the adoption of public cloud for FIs — 6

Recommendation 2:
Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services — 6

Recommendation 3:
Regulations should not require regulator's prior approval for implementation of cloud services for each workload — 6

Recommendation 4:
Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal — 6

Recommendation 5:
Regulations should have a clear distinction between control vs processing of data — 6

Recommendation 6:
Regulations should permit cross-border data transfers and should not require data to be stored in a specific geography — 6

Recommendation 7:
Regulations should not prescribe terms of cloud contracts — 6

Recommendation 8:
Regulations should not create a right to government unrestricted physical audit access to CSP facilities — 6

Recommendation 9:
Regulations and regulators are neutral as to foreign or domestic CSPs — 6

Recommendation 10:
Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors — 6

TOTAL SCORE (max 60): 60

Market overview and key updates

Both the Financial Conduct Authority (FCA) and the Prudential Regulatory Authority (PRA) are responsible for the financial sector within the UK, although for the purposes of banking services, the FCA is the primary regulator.

A major recent upheaval for the UK has been the implications of the UK's exit from the European Union (Brexit), which is scheduled to be completed by 31 Dec 2020.[393] This has implications for data management regulations, as many regulatory documents still currently point to or refer to EU legislation, such as the General Data Protection Regulation (GDPR)[394] and take reference from these regulations. It is still unclear what will happen following Brexit, and this is translating into increased compliance costs as financial businesses grapple with regulatory uncertainty as the market navigates this transition. The Information Commissioner's Office (ICO) has attempted to provide information on the transition, but as they note on their website, developments and further regulatory clarity will have to wait "until the end of 2020 to allow time to negotiate a new relationship with the EU."[395]

The FCA has structured its approach towards managing risk and providing guidance to the industry for outsourcing and cloud computing technology. Its primary guideline document is the FCA Handbook,[396] where the Senior Management Arrangements, Systems and Controls Sourcebook (SYSC) 7 is on Risk Control, and SYSC 8 provides specific information on outsourcing arrangements.

In addition, the FCA has specifically called out Outsourcing and Operation Resilience in a webpage[397] which explains their stance towards various aspects of outsourcing, along with the relevant links. This "sense-

393 BBC (2020) Brexit: What you need to know about the UK leaving the EU, https://www.bbc.com/news/uk-politics-32810887
394 EC EU Data Protection Rules, https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en
395 Information Commissioner's Office, Data Protection after the end of the transition period, https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/
396 FCA, Handbook, https://www.handbook.fca.org.uk/handbook/SYSC/8/
397 FCA, 2020, Outsourcing and operational resilience https://www.fca.org.uk/firms/outsourcing-and-operational-resilience

making page" also includes links to external websites with related and relevant information, such as the Information Commissioner's Office, the PRA, National Cyber Security Center, and other related document links.

Relevant Regulators

- Financial Conduct Authority (FCA)[398]
- Prudential Regulation Authority (PRA)[399]
- (until 31 Dec 2020) European Banking Authority (EBA)[400]
- Information Commissioner's Office (ICO)[401]

Relevant Regulations

- FCA Handbook: Senior Management Arrangements, Systems and Controls Sourcebook (SYSC)[402]
- FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services[403]

Summary of market alignment with the recommendations

Regulatory Recommendations	UK's Scores and Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**6 points: Yes, public cloud adoption is promoted in a public affirmation.** This public affirmation is implied in the 2016 FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services.[404]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**6 points: Yes, regulations set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption (could be through a reference in the regulation itself or in accompanying cloud computing guidelines/ information papers). Such processes are proportionate, practical and not unduly burdensome.** Yes, FG 16/5 provides a clear process,[405] pointing to the processes in the SYSC which will determine any outsourcing arrangement, including adopting cloud computing.[406]
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**6 points: No regulator's approval necessary – (compliance with global standards and international third-party certifications are sufficient).** No explicit cloud approvals are necessary, as the approach taken by the FCA is one where financial firms are required to undertake a risk management approach when outsourcing, focusing on operational resilience.[407] However, the FCA has a notification requirement for FIs who wish to enter into a material outsourcing arrangement, as detailed in SYSC 13.[408]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**6 points: Yes, regulations clearly differentiate applicability to material and non-material workloads, and regulations for non-material workloads are light touch (minimal), if any. Criteria for assessing materiality are clearly defined.** Yes, FG 16/5 differentiates between critical, important, and material.[409] This differentiation is also noted in SYSC 12 on Group risk systems and controls requirements in a light-touch manner.[410]
5. Regulations should have a clear distinction between control vs processing of data	**6 points: Yes, there is a clear distinction between an entity that is a controller versus one that is a processor of data.** Prior to the UK's exit from the EU on 31 Jan 2020, it was subject to the EU's General Data Protection Regulations (GDPR),[411] which makes this distinction between the data controller and data processor. This distinction still holds true while the UK's exit from the EU is still in a transitional phase, which will last until 31 Dec 2020.[412]
6. Geographic Restrictions:	

398 Financial Conduct Authority, https://www.fca.org.uk
399 Professional Financial Claims Association, https://www.pfca.org.uk
400 European Banking Authority, https://eba.europa.eu
401 Information Commissioner's Office, https://ico.org.uk
402 FCA, Handbook, https://www.handbook.fca.org.uk/handbook/SYSC
403 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
404 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it
405 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
406 FCA, Handbook, https://www.handbook.fca.org.uk/handbook/SYSC
407 FCA, 2020, Outsourcing and operational resilience, https://www.fca.org.uk/firms/outsourcing-and-operational-resilience
408 FCA, Handbook, https://www.handbook.fca.org.uk/handbook/SYSC
409 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
410 FCA, Handbook, https://www.handbook.fca.org.uk/handbook/SYSC
411 CNBC, January 2020, UK formally leaves the European Union and begins Brexit transition period, https://www.cnbc.com/2020/01/31/brexit-day-uk-formally-leaves-the-european-union.html
412 ICO, Data Protection at the end of the transition period, https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/

Regulatory Recommendations	UK's Scores and Justifications
a. Regulations should permit the cross-border transfer of data	**3 points: Yes, cross-border transfers are allowed with appropriate safeguards.** Yes, cross-border transfer of data is permitted. Prior to the UK's exit from the EU on 31 Jan 2020,[413] it was subject to the EU's General Data Protection Regulations (GDPR), which stipulates data protection for the transfer of data outside of EU jurisdiction. In addition, the transfer of EU citizens' data was subject to the EU-US Privacy Shield Agreement; however, this struck down on 16 Jul 2020, leaving cross-border transfers of data permissible and governed under Standard Contractual Clauses (SCC). While the UK's exit from the EU is still in a transitional phase (which will last until 31 Dec 2020),[414] the details on cross-border data transfers are still likely permitted under Standard Contractual Clauses (SCC).
b. Regulations should not require data to be stored in a specific geography	**3 points: No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** Regulations do not require data to be stored in a specific jurisdiction, only for firms to "ensure that data is not stored in jurisdictions that may inhibit effective access to data for UK regulators."[415]
7. Regulations should not prescribe terms of cloud contracts	**6 points: Yes, regulations are not prescriptive as to terms of a cloud contract.** The SYSC[416] does require contractual arrangements to observe the right of the FCA to exercise its regulatory authority and oversight of the financial institution, but there are no regulations which prescribe the terms of cloud contracts specifically.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**6 points: There is no regulatory requirement of a right to unrestricted physical access for audit, and as to audit, it is clear that regulators and FIs can rely on third-party reports.** Yes, FG 16/5 provides instructions on a limited approach towards physical audit and access rights to FSI data under access to business premises.[417]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**6 points: Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** The FCA's guidance through FG 16/5 does not stipulate separate or additional requirements for FIs outsourcing to foreign service providers.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**6 points: Regulations promote a risk-based approach to operational resiliency AND include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors. Further, regulations are not prescriptive.** Yes, FG 16/5 is a non-prescriptive guiding document, and has specific sections addressing Risk Management, Exit Plans, with notes on managing exit plans, transiting to alternative service providers, and managing other forms of risk.[418]

413 CNBC, January 2020, UK formally leaves the European Union and begins Brexit transition period, https://www.cnbc.com/2020/01/31/brexit-day-uk-formally-leaves-the-european-union.html
414 EPC, 2020, Brexit from 1 January 2021 onwards: get ready for the end of the transition period, https://www.europeanpaymentscouncil.eu/news-insights/news/brexit-1-january-2021-onwards-get-ready-end-transition-period, https://www.fca.org.uk/firms/preparing-for-brexit/uk-banking-payment-sectors
415 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
416 FCA, Handbook, https://www.handbook.fca.org.uk/handbook/SYSC
417 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
418 FCA, FG 16/5, Guidance for firms outsourcing to the 'cloud' and other third-party IT services, https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

United States of America (USA)

Market overview and key updates

The regulatory structure for the US financial services industry is relatively complex in comparison to other markets, given oversight at both the federal and state level with respective rules and regulations.

Federal Level Regulators

Adding to the complexity is the presence of several regulators at the federal level who have varying levels of oversight of FIs. These regulators include the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), and the Federal Deposit Insurance Corporation (FDIC). For the purposes of this report, the OCC is considered the primary regulator for the banking sector.

All three are also members of the Federal Financial Institutions Examination Council (FFIEC), an interagency body of financial sector regulators that is tasked with drafting principles and standards to promote uniformity across all US financial institution regulators.[419] Since at least 2012, the FFIEC has taken the stance that cloud computing is no different from other forms of outsourcing.[420] As such, cloud usage falls under the FFIEC's Outsourcing Technology Services Booklet, an online document containing guidance and requirements for FIs looking to use third party service providers to meet their technology needs.[421]

State Level Regulators: New York State Department of Financial Services (NYDFS)

At the state level, this report uses New York State, considered the financial center of the US, as an illustrative example. The primary regulator for New York is the New York State Department of Financial Services (NYDFS), which has built up a reputation as a leader in addressing technology innovation in the financial sector. For example, in 2015, NYDFS released the first state licensing framework for virtual currencies,[422] and in 2019, NYDFS announced the creation of a Research and Innovation Division to help the regulator adapt to fintech developments.[423] In terms of technology outsourcing, NYDFS has set the bar in the US for issuing ground-breaking regulations on Cybersecurity Requirements for Financial Services Companies in March 2017, which are intended to protect information systems and non-public information from cybersecurity risks. [424]

Selected relevant regulators

- Federal: Office of the Comptroller of the Currency (OCC)
- Federal: Federal Financial Institutions Examination Council (FFIEC)
- State: New York State Department of Financial Services (NYDFS)

Relevant regulation(s)

- FFIEC, Outsourced Cloud Computing[425]
- FFIEC, Joint Statement on Security in a Cloud Computing Environment[426]
- FFIEC, Outsourcing Technology Services Booklet[427]
- Bank Service Company Act[428]
- Gramm-Leach-Bliley Act[429]

419 FFIEC, https://www.ffiec.gov/
420 FFIEC, 2012, Outsourced Cloud Computing, https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
421 FFIEC, Outsourcing Technology Services Booklet, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
422 NYDFS, 2015, NYDFS Announces Approval of First BitLicense Application From a Virtual Currency Firm, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1509221
423 Pillsbury Winthrop Shaw Pittman LLP, 2019, New York DFS Creates New FinTech Division, https://www.pillsburylaw.com/en/news-and-insights/new-york-dfs-creates-new-fintech-division.html
424 NYDFS, 2019, DFS Superintendent Vullo Advises Regulated Entities of Final Deadline for Implementing Protections Under DFS's Landmark Cybersecurity Regulation, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1901311
425 FFIEC, 2012, Outsourced Cloud Computing, https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
426 FFIEC, 2020, Joint Statement on Security in a Cloud Computing Environment, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf
427 FFIEC, Outsourcing Technology Services Booklet, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
428 Bank Service Company Act, https://ithandbook.ffiec.gov/media/27536/con-12usc1861_1867c_bank_service_company_act.pdf
429 Gramm-Leach-Bliley Act, https://www.ffiec.gov/exam/infobase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf

- OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance[430]
- OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29[431]
- 23 New York Codes, Rules and Regulations (NYCRR) 500, NYDFS Cybersecurity Requirements for Financial Services Companies[432]
- NYDFS Supervisory Policy G101[433]

Summary of market alignment with the recommendations

Federal: Office of the Comptroller of the Currency (OCC)

Regulatory Recommendations	USA (OCC federal law) Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**Yes, public cloud adoption is promoted in a public affirmation.** In 2012, the Federal Financial Institutions Examination Council (FFIEC), which consists of the Federal Reserve Bank and the Office of the Comptroller of the Currency (OCC), among others, issued a document on "Outsourced Cloud Computing" noting benefits of cloud and that they consider the cloud to be another form of outsourcing with the same basic risks as other forms of outsourcing.[434] The US Department of the Treasury has also advocated for facilitation of cloud usage and other technologies in financial services.[435]
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**Yes, regulations set out a clear process for FIs to follow when entering into an outsourcing arrangement (e.g. conducting due diligence, assessing risks, notifying regulator) and it is explicit that this process also applies to cloud adoption (could be through a reference in the regulation itself or in accompanying cloud computing guidelines/ information papers). Such processes are proportionate, practical and not unduly burdensome.** The FFIEC has an Outsourcing Technology Services Booklet detailing the procedure and requirements to follow when outsourcing technology, which the FFIEC has separately stated is applicable to the cloud.[436] These requirements include risk assessment, due diligence, and ongoing monitoring of the relationship with the service provider, among others.
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**No regulator's approval necessary – (compliance with global standards and international third-party certifications are adequate).** The FFIEC Outsourcing Technology Services Booklet does not mention any requirement for government approval. However, under the Bank Service Company Act, there is a notification requirement for certain outsourcing relationships within 30 days of the start of the contract,[437] which regulators have interpreted to include data processing and Internet banking services.[438] As part of this notification requirement, the OCC requires "a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the bank" per OCC Bulletin 2013-29.[439]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**Yes to an extent.** The OCC defines critical activities as those that include significant bank functions or significant shared services, or other activities that could cause a bank to face significant risk if a third party fails to meet expectations, etc. The OCC notes that it expects "more comprehensive and rigorous oversight and management for third party relationships involving critical activities"[440] and provides guidance in how to manage risk and meet compliance objectives for all third party service provider relationships in general. (With the exception of requirements such as board approval for third party contracts involving critical activities, the requirements between critical and non-critical activities are largely the same.)
5. Regulations should have a clear distinction between control vs processing of data	**Unclear or ambiguous.** OCC regulations do not explicitly define control or processing of data or assign responsibilities as a result of a party controlling or processing data. In effect, however, the regulations assign the role of the data controller to the financial institution. For example, the FFIEC issued a Joint Statement on Security in a Cloud Computing Environment in 2020, which stipulates that "the financial institution retains overall responsibility for the safety and soundness of cloud services and the protection of sensitive customer information."[441] The OCC also issued OCC Bulletin 2020-10 on third party risk management, which notes that

430 OCC, 2013, Bulletin 2013-29, https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
431 OCC, 2020, Bulletin 2020-10, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html
432 NYDFS, 2017, 23 NYCRR 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf
433NYDFS, Supervisory Policy G101, https://govt.westlaw.com/nycrr/Document/I4e7c3e14cd1711dda432a117e6e0f345?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)
434 FFIEC, 2012, Outsourced Cloud Computing, https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
435 US Department of the Treasury, A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation, 2018, https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf
436 FFIEC, Outsourcing Technology Services Booklet, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
437 Bank Service Company Act, https://ithandbook.ffiec.gov/media/27536/con-12usc1861_1867c_bank_service_company_act.pdf
438 American Bankers Association, Bank Service Company Act, https://www.aba.com/banking-topics/compliance/acts/bank-service-company-act
439 OCC, 2013, Bulletin 2013-29, https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
440 OCC, 2013, Bulletin 2013-29, https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
441 FFIEC, 2020, Joint Statement on Security in a Cloud Computing Environment, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf

Regulatory Recommendations	USA (OCC federal law) Justifications
	the bank is ultimately responsible for the effectiveness of the control environment regardless of the division of control responsibilities.[442]
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**Yes, cross-border transfers are allowed with appropriate safeguards.** Neither FFIEC nor OCC regulations explicitly restrict cross-border data transfer. However, FFIEC notes that regulated entities which use foreign-based third party service providers (or domestic service providers that subcontract to foreign-based firms) must comply with applicable US laws such as Section 501(b) of the Gramm-Leach-Bliley Act (GLBA) which stipulates safeguards for customer data[443] and export control regulations for encryption software, hardware, and network applications. In addition, FFIEC notes that regulated entities should account for foreign data privacy laws and regulatory requirements.[444]
b. Regulations should not require data to be stored in a specific geography	**No there are no requirements that data be stored in a specific geography, so long as there are appropriate safeguards.** Neither FFIEC nor OCC regulations explicitly require data localization, and regulated entities are required to comply with applicable US and foreign laws as noted above.
7. Regulations should not prescribe terms of cloud contracts	**Yes, regulations are not prescriptive as to terms of a cloud contract.** FFIEC's outsourcing guidance sets out areas for consideration and items regulated entities should address within their Service Level Agreements with technology service providers but does not prescribe specific terms that must be contained within contracts. [445] FFIEC's cloud-specific rules also provide high-level topics for entities to consider in their cloud contracts.[446]
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**No unrestricted physical audit right. It is clear that regulators and FIs can rely on third-party reports**. FFIEC's cloud joint statement recommends the use of auditors and explicitly states that independent assurance reviews constitute oversight and monitoring. In addition, this guidance mentions that a regulated entity's management may test a CSP's controls if permitted by the contract; if not, the entity's management can use the system and organizational control (SOC) reports, ISO certifications, and independent assurance reviews.[447] OCC guidance also notes that SOC reports suffice in lieu of on-site audits.[448]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**Regulators and regulations do not distinguish between domestic CSPs and foreign CSPs.** The FFIEC does not explicitly discriminate against foreign CSPs and contains guidance on the use of foreign-based third party service providers in its outsourcing booklet. The FFIEC notes that regulated entities should ensure that the use of a foreign service provider does not violate any applicable US laws (e.g. GLBA and the Bank Secrecy Act) and that entities should also take into account other US regulations such as sanctions and embargos from the US Treasury Department's Office of Foreign Assets Control (OFAC) and encryption-related export restrictions. In addition, FFIEC stipulates that "An organization's use of a foreign-based third-party service provider (and the location of critical data and processes outside of U.S. territory) must not compromise the ability of U.S. regulatory authorities to effectively examine the organization."[449] However, the US Department of State has separately launched the Clean Network program which aims to protect American privacy by restricting the use of Chinese technology. In August 2020, the program was extended to include "Clean Cloud" to prevent data storage and processing that could be accessible to the Chinese government through companies such as Alibaba, Baidu, and Tencent.[450]
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	**Regulations promote a risk-based approach to operational resiliency AND provide non-mandatory guidance to encourage FIs to look at factors such as geographic diversity, reversibility and exit planning, and vendor choice and are not prescriptive.** FFIEC's cloud joint statement takes a principles-based approach to risk management and resiliency, and provides guidance to regulated entities to consider exit planning and geography as part of cloud security management. In addition, the statement specifically refers to interoperability and portability as controls unique to cloud computing services, which a regulated entity can consider depending on its risk appetite.[451]

442 OCC, 2020, Bulletin 2020-10, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html
443 Gramm-Leach-Bliley Act, https://www.ffiec.gov/exam/infobase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf
444 OCC, Outsourcing Technology Services Booklet, Appendix C: Foreign-Based Third-Party Service Providers, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-c-foreign-based-third-party-service-providers.aspx#cite-text-0-5
445 OCC, Outsourcing Technology Services Booklet, Key Service Level Agreements and Contract Provisions, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/ongoing-monitoring/key-service-level-agreements-and-contract-provisions.aspx. See also OCC, Outsourcing Technology Services Booklet, Service Level Agreements (SLAs), https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/contract-issues/service-level-agreements-(slas).aspx
446 FFIEC, 2020, Joint Statement on Security in a Cloud Computing Environment, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf
447 FFIEC, 2020, Joint Statement on Security in a Cloud Computing Environment, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf
448 OCC, 2020, Bulletin 2020-10, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html
449 OCC, Outsourcing Technology Services Booklet, Appendix C: Foreign-Based Third-Party Service Providers, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-c-foreign-based-third-party-service-providers.aspx#cite-text-0-4
450 US Department of State, 2020, Announcing the Expansion of the Clean Network to Safeguard America's Assets, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/
451 FFIEC, 2020, Joint Statement on Security in a Cloud Computing Environment, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf

Illustrative State: New York Department of Financial Services

Regulatory Recommendations	USA (New York State law) Justifications
1. Governments have publicly affirmed the adoption of public cloud for FIs	**No mention of financial sector using cloud.** The New York State Department of Financial Services (NYDFS) does not appear to have made any public affirmations on public cloud adoption.
2. Regulations should set out a clear and not unduly burdensome process for FIs to follow when adopting cloud services	**No, there is no clear process or regulatory guidance on outsourcing or cloud adoption.** NYDFS has Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500) which lay out requirements such as risk assessments, cybersecurity policy formulation, and third party service provider security policies.[452] However, these regulations do not mention cloud.
3. Regulations should not require regulator's prior approval for implementation of cloud services for each workload	**No regulator's approval necessary.** NYDFS regulations only stipulate notification requirements. For example, NYDFS Supervisory Policy G101 requires notification when a regulated entity decides to contract automated data processing services.[453]
4. Regulations should be risk-based and clearly differentiate applicability to material and non-material workloads; and for non-material workloads, requirements should be minimal	**No differentiation and all workloads are treated equally.** 23 NYCRR 500 does not explicitly differentiate between material and non-material workloads. The regulations broadly emphasize protection of information systems and customer information for all regulated entities.[454]
5. Regulations should have a clear distinction between control vs processing of data	**Unclear or ambiguous**. Although 23 NYCRR 500 does not explicitly distinguish between control vs. processing of data. However, the regulations make clear that the onus is on the regulated entity to develop a cybersecurity policy which includes third party service provider management, and to implement a third-party service provider security policy. [455] In other words, regulated entities are responsible for setting the standards and maintaining cybersecurity of data that may reside with a third-party service provider.
6. Geographic Restrictions:	
a. Regulations should permit the cross-border transfer of data	**There are no geographic restrictions.** NYDFS regulations, namely 23 NYCRR 500, do not explicitly contain any restrictions on cross-border data transfer or require data localization.
b. Regulations should not require data to be stored in a specific geography	
7. Regulations should not prescribe terms of cloud contracts	**Yes, regulations are not prescriptive as to terms of a cloud contract.** Supervisory Policy G101 stipulates that contracts for automated data processing services should state that the regulator has the right to examine all records and material, use the equipment, and interview employees insofar as needed to protect the interests of those receiving the services. [456] However, 23 NYCRR 500 (the key operative document on technology outsourcing) identifies compliance objectives and areas to address vis a vis cybersecurity for regulated entities. Specifically, the regulations note that regulated entities need to have written policies or procedures that include due diligence and/or contractual provisions to address issues such as: third party service provider access controls, including multi-factor authentication, and third party service provider use of encryption. It is not explicit, however, that such provisions must be contained within an SLA/cloud contract.
8. Regulations should not create a right to government unrestricted physical audit access to CSP facilities	**Unclear or ambiguous. It is not clear if regulations require the CSP to provide the regulator with unrestricted physical access.** Supervisory Policy G101 indicates that the regulator has the "right to examine all records and material, use the equipment and interview employees of the firm or banking organization" providing automated data processing services.[457] In addition, 23 NYCRR 500 mentions that periodic assessments of third party service providers are needed depending on the risk the service provider presents and the continued adequacy of their cybersecurity practices; it is not explicitly mentioned anywhere that unrestricted physical access rights should be granted to the regulator.[458]
9. Regulations and regulators are neutral as to foreign or domestic CSPs	**No preferences for domestic CSPs over foreign CSPs.** 23 NYCRR 500 does not explicitly distinguish between domestic and foreign service providers, or otherwise require local registration for service providers.
10. Regulations promote a risk-based approach to effective operational resiliency, which may include non-mandatory guidance encouraging the FI to	**Regulations promote a risk-based approach to operational resiliency and are not prescriptive, but do not provide non-mandatory guidance to encourage FIs to look at factors such as geographic diversity, reversibility, exit planning, and vendor choice.** 23 NYCRR 500 approaches cybersecurity

452 NYDFS, 2017, 23 NYCRR 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf
453 NYDFS, Supervisory Policy G101, https://govt.westlaw.com/nycrr/Document/I4e7c3e14cd1711dda432a117e6e0f345?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)
454 NYDFS, 2017, 23 NYCRR 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf
455 NYDFS, 2017, 23 NYCRR 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf
456 NYDFS, Supervisory Policy G101, https://govt.westlaw.com/nycrr/Document/I4e7c3e17cd1711dda432a117e6e0f345?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)
457 NYDFS, Supervisory Policy G101, https://govt.westlaw.com/nycrr/Document/I4e7c3e17cd1711dda432a117e6e0f345?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)
458 NYDFS, 2017, 23 NYCRR 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

Regulatory Recommendations	USA (New York State law) Justifications
consider business continuity and disaster recovery planning, geographic diversity, reversibility, exit planning, and vendor choice, among other factors	from a risk-based approach to allow regulated entities to assess and address risk according to the entity's profile, but does not explicitly address tools such as reversibility, interoperability, etc..[459]

459 NYDFS, 2017, 23 NYCRR 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

Appendix: How Cloud Business Models Affect Regulatory Compliance

Shared Responsibility Model

In adopting cloud computing, the customer (an FI) and the CSP share responsibility for security. This model of 'shared responsibility' allocates responsibility to the entity that has control over the data (typically the FI, or 'data controller') and the processor of the data, the CSP. CSPs are responsible for the security of the cloud and customers are responsible for security in the cloud (securing the data they put in the cloud). In practical terms, at a minimum (e.g., Infrastructure as a Service (IaaS)) this means the CSP is responsible for the security of its facilities (virtual and physical security of the servers, networks and buildings), and the customer (often called the data controller) is responsible for all other security. This can progress along a continuum, where the FI contracts more responsibility to the CSP, depending on the services being provided by the CSP. But invariably, both share responsibility for security.

To put this in terms of compliance, at the foundational level of providing IaaS, the CSP is responsible for maintaining and proving the regulatory compliance of the cloud, while customer FIs are required to maintain and prove regulatory compliance of the data and applications they host in the cloud. CSPs may offer security controls as a service to their customers, making it easier for the FI customer to simply select and manage security controls for their data and applications hosted on the CSP's cloud. In these circumstances, the FI maintains control over its data and applications, including how it uses the security controls made available by the CSP. Again, this is in the context of IaaS, and as services expand to providing Platform as a Service (PaaS), or further 'up the stack' to provide applications (Software as a Service (SaaS), the responsibilities for compliance fall to the customer and CSP according to their contract in alignment with the control being exercised by the entity.

International Certifications and Assurance Standards

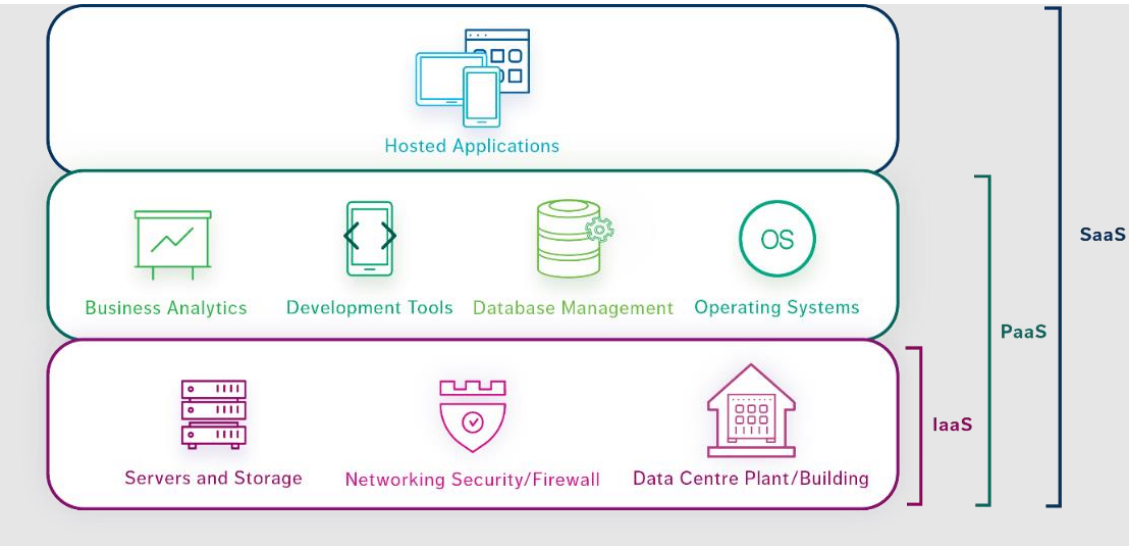
One important way of assuring compliance is through certifications to recognized international standards. AWS, Google, Microsoft and the other major CSPs make information regarding their achieved compliance certifications readily available to all their customers. These all maintain several recognized industry certifications to industry standards such as Statement on Standards for Attestation Engagements' (SSAE) Standard Occupational Classification standards SOC 1, SOC 2 and SOC 3, and International Standards Organization's standards ISO 27001, ISO 27017, and ISO 270187. A SOC 2 assessment will reveal how the CSP is compliant with the Gramm-Leach-Bliley Act (GLBA).[460]

Three Types of Cloud

The three common models of cloud service provisioning are the traditional 'Infrastructure as a Service' (IaaS) and the more elaborate 'Platform as a Service' (PaaS) and 'Software as a Service' (SaaS). In each case, the CSP has less (IaaS) or somewhat more (PaaS) responsibility in how it protects an FIs data and applications. In each case, the Service Level Agreement (SLA) will dictate who is responsible for particular aspects of security (and in this way, compliance). In all cases, the FI is ultimately responsible to the regulator, but some of the compliance functions or activities are undertaken by the CSP. The regulator must understand when the FI is contracting certain responsibilities to the CSP, and enable such a delegation (to be clear, without abrogating their responsibility for compliance, typically through oversight of the CSP's compliance with the SLA).

460 Particularly, Section 501(b) of the GLBA, which requires financial institutions to establish appropriate "administrative, technical, and physical safeguards" to protect the security and confidentiality of their customers' "non-public personal information".

Figure 21: Three Common Models for Cloud Provisioning



Source: TRPC Research, 2021

Infrastructure as a Service (IaaS)

The fundamental public cloud service is the provision of infrastructure, the data center housing the servers and storage (compute power and capacity), networking, and security and firewalls for this infrastructure. A CSP which provides IaaS has no control of or access to the data or applications running on the infrastructure. For example, the CSP cannot access the customer's data because the customer has security controls in place, including access controls and encryption and the CSP cannot circumvent the customer's access controls, nor decrypt data that a customer encrypts before sending the data to the cloud servers. The responsibility for protecting the data is defined by the CSP's protection of the anonymous bits of data on the servers and the networks that are within their control.

Platform as a Service (PaaS)

Sitting atop the infrastructure, some CSPs provide additional services, typically an operating system and developers tools with which the CSP's customer can build applications. With the operating system, PaaS gives customers tools to build applications to meet their own specifications and needs. Some tools may be analytics or business intelligence tools that can mine a business's data to find insights and patterns to predict outcomes. Again, these tools provide capabilities for a customer to design applications that will help the customer improve forecasting, design products, make investments or other business decisions. The benefit of these services is that a CSP's customer can develop applications with fewer resources, building with universal tools that will serve a range of needs for the customers of the CSP. These tools also have built-in efficiencies, for example, enabling the CSP customer to develop an application that will run on a range of platforms, such as desktop or mobile devices. The services are priced at a pay-as-you-go service rate, so the customer only pays while using the service. Finally, the agile environment enables the customer to design and support an app throughout its lifecycle, from building to testing and deploying, managing and updating in the same environment.

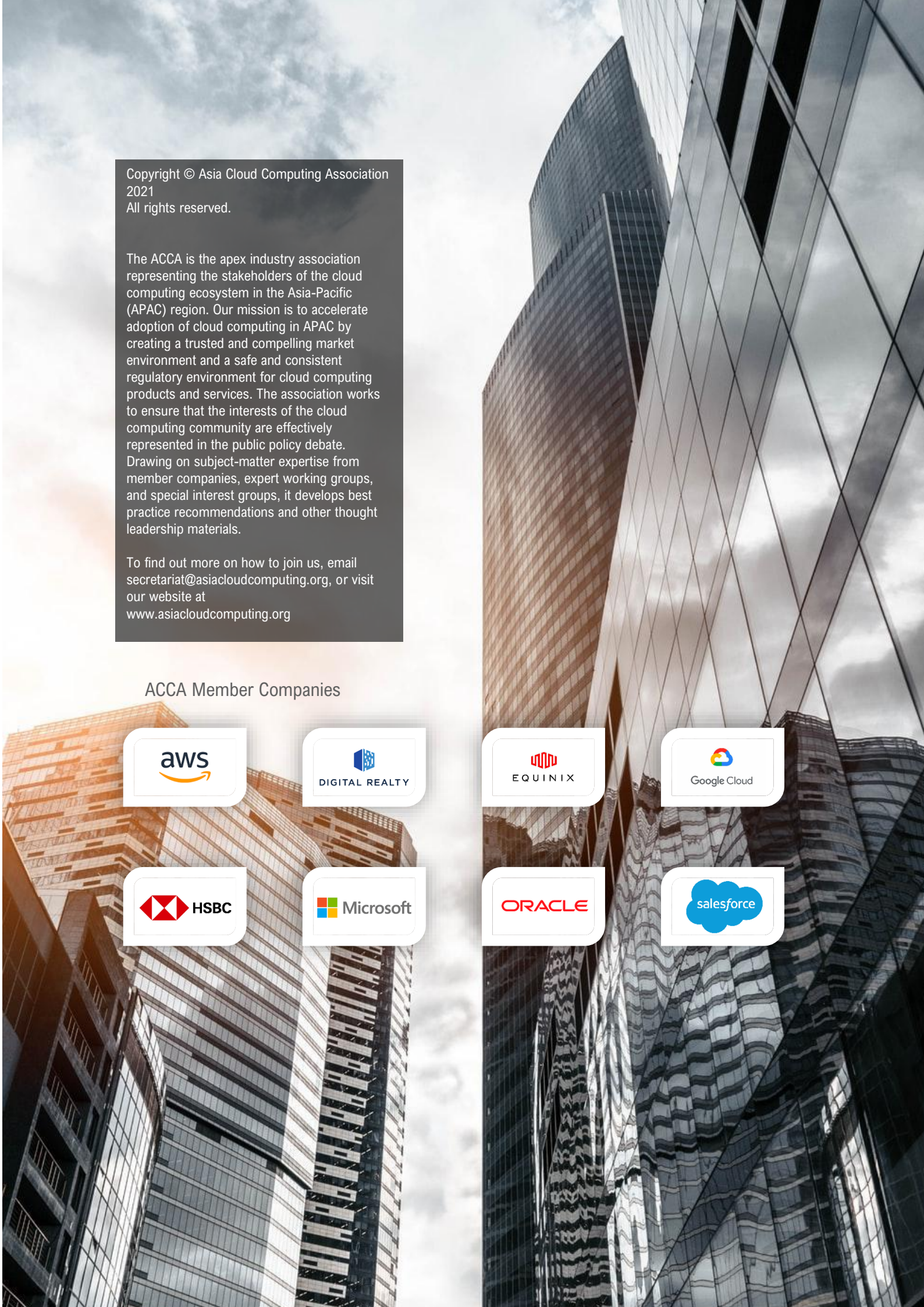
In the context of PaaS, the Service Level Agreement (SLA) will allocate responsibility for security, audit, and other compliance obligations of the FI. Typically, the CSP is responsible for the virtual and physical security of its software, hardware, network and facilities. The SLA may provide for more security controls for the customer's data, some of which may be controlled by the customer, some by the CSP, depending on the terms of the SLA.

Software as a Service (SaaS)

With Software as a Service (SaaS), in addition to the infrastructure and platform, the CSP also provides software applications, such as accounting, database or relationship management software. Gmail, Microsoft 365 productivity and Salesforce Customer Relations Management (CRM) software are all examples of SaaS. Some CSP's offer unbranded 'white-label' software to a SaaS customer to be branded by the customer, or integrated into their branded website or app. An example of a white label application that may be procured by an FI is software for customer support, such as a platform that manages chats, emails or call center support, or online maps, video capabilities, geographic maps, social media integration or other services or functionality that is integrated into an FI's website or app. With SaaS, the FI's data generally resides on the CSPs servers.

Many SaaS applications are web browser based or apps and run on a range of devices, which makes the use of SaaS appealing to a CSP's customers, in that the CSP develops, manages and updates the software. Unlike traditional software, which is purchased and upgraded for a fee, SaaS is a subscription service that includes all upgrades and updates. The benefit is that SaaS software is always up to date with security patches without any effort by the customer, so enterprise support for the software is a lessened cost.

In the context of SaaS, the responsibility for compliance remains with the FI, but the SLA provides for security controls for the customer's data at the application level, some of which may be controlled by the FI (e.g., password protected access controls), some by the CSP, depending on particular software and the terms of the SLA. Even in the context of SaaS, the CSP is responsible for the security of its software, hardware, network and facilities.



The ACCA is the apex industry association representing the stakeholders of the cloud computing ecosystem in the Asia-Pacific (APAC) region. Our mission is to accelerate adoption of cloud computing in APAC by creating a trusted and compelling market environment and a safe and consistent regulatory environment for cloud computing products and services. The association works to ensure that the interests of the cloud computing community are effectively represented in the public policy debate. Drawing on subject-matter expertise from member companies, expert working groups, and special interest groups, it develops best practice recommendations and other thought leadership materials.

To find out more on how to join us, email secretariat@asiacloudcomputing.org, or visit our website at www.asiacloudcomputing.org

ACCA Member Companies

aws
DIGITAL REALTY
EQUINIX
Google Cloud
HSBC
Microsoft
ORACLE
salesforce