NOVEMBER 2021

CLOUD ADOPTION AND REGULATION IN ASIA-PACIFIC FINANCIAL SERVICES

INSTITUTE OF INTERNATIONAL FINANCE

Institute of International Finance

Acknowledgements

IIF would like to thank those central banks, monetary authorities, bank supervisors and securities regulators in region (including both IIF members and non-members) who engaged with our staff around these topics. They were: Australian Prudential Regulation Authority; Australian Securities and Investments Commission; Reserve Bank of Australia; Hong Kong Securities and Futures Commission; Hong Kong Monetary Authority; Bank Indonesia; Otoritas Jasa Keuangan (Indonesian Financial Services Authority); Reserve Bank of India; Bank of Japan; Japan Financial Services Agency; Bank Negara Malaysia (Malaysian Central Bank); Bangko Sentral ng Pilipinas (Philippines Central Bank); Monetary Authority of Singapore; Bank of Thailand; and State Bank of Vietnam.

We also wish to thank those IIF member financial institutions who contributed to the Steering Committee to oversee the project, and to the focus groups and bilateral discussions whose insights and input have contributed to this report.

IIF acknowledges the support of Amazon Web Services, Inc. in sponsoring the production of this report.

Table of contents

1 Overview

The Asia-Pacific region is the world's fastest growing economy by many measures. Cloud computing is one of the more rapidly growing markets globally, and has entered the financial services sector strongly. It is therefore timely for the Institute of International Finance (**IIF**) to take stock of cloud adoption and regulation trends in Asia-Pacific by surveying attitudes and settings at financial institutions (**FIs**) and at central banks and regulators. As well as reporting back on attitudes and trends, this report aims to show how regulatory settings can act as a facilitator for cloud adoption, and to identify the key emerging regulatory issues under discussion by FIs and regulators in region and globally. It closes with some recommendations around cloud adoption for FIs, regulators and other stakeholders.

1.1 Key findings

Our key findings from our engagement with authorities and FIs are as follows:

Cloud adoption by FIs is increasing, and in some cases accelerating. Many authorities have seen FIs migrate non-core services, and several authorities now oversee cloud-native FIs, while fewer have seen mainly smaller banks migrating core services to the cloud.

Benefits of adoption include improved security and cost savings. FIs, particularly smaller ones, stand to benefit from the increased sophistication of cyber defenses and patching at cloud service providers (**CSPs**), while authorities warn misconfiguration risk management is key. FIs expect substantial reductions in cost from cloud migration, as well as more flexibility in budgeting.

Talent is crucial. Recruiting and retaining talent is an issue, particularly granular expertise around cloud migration and particular CSP offerings. Regulators are encouraging FIs to reskill existing workforces to meet this challenge, and CSPs are offering more courseware to assist.

No authority sees an immediate need to extend the regulatory perimeter to cover CSPs, and systemic risk is not considered significant at this time. Most regulators see their role as ensuring that FIs manage the risks of cloud adoption, rather than the business risk of *not* adopting cloud. Data sharing and access, systemic and concentration risk and cooperative supervision are among the topics where authorities feel more international coordination would be helpful.

There is a variety of attitudes among authorities to data localization, but all regulators insist that access to data is vital, while data localization remains a key "pain point" for FIs. Some jurisdictions require that encryption keys remain local even if data is held remotely. Authorities often make an exception from data localization rules for foreign-headquartered banks. A variety of rationales are cited for data localization rules where present. For FIs, data localization rules were the key regulatory barrier cited. These rules limit the benefits of scale that cloud can bring, increase cyber risk, and reduce or eliminate the scope for data aggregation, thus limiting the ability to accurately model global risk and also the effectiveness of anti-fraud or anti-money laundering (**AML**) systems.

1.2 Key recommendations

Many FIs are hesitant about cloud adoption because of mixed regulatory signals, risk concerns, and the initial costs. While these are risks to understand and mitigate, the transformational benefits of shifting from a closed archaic IT system to cloud have become essential.

In the IIF's view, the business risks to FIs of not adopting cloud are greater than the risks posed by cloud, due also to the competitive threat to regulated FIs from cloud-enabled BigTechs and fintechs, in an environment of heightened user expectations, reduced margins and, for the present, cheap capital.

FIs and regulators should therefore adopt approaches that help smooth the transition to the technology, while always ensuring that risks are adequately monitored and managed.

Data localization requirements are frequently not the best means to achieve regulatory objectives. Clearly identifying objectives and working with industry can yield better results for the entire economy.

FIs should focus on developing an adoption plan based on their institution's strategic goals and objectives consistent with their risk management strategies.

Financial institutions and regulators working closely together could enable safe and successful migration, chiefly by providing clear guidance and timely and easy to navigate notification/approval processes.

This paper contains further detailed recommendations and a more in-depth discussion of data localization requirements in section 5, and issues for further study in section 6.

1.3 Methodology

The report's findings are based on written or oral interviews with senior representatives of 15 official sector agencies (central banks, monetary authorities, bank supervisors and securities regulators) across 10 Asia-Pacific economies.[1] The IIF also held focus groups and bilateral discussions with FI members based or active in the region and engaging with cloud adoption issues. Those engagements were conducted in September – November 2021. We also conducted a literature review, building on the IIF's own prior publications on cloud[2] and the IIF – Deloitte series on digital transformation.[3]

For the purposes of this Report, "**cloud adoption**" covers: the migration of FI legacy systems/workloads to the cloud; the advent of cloud-native FIs; and traditional FIs rolling out new cloud-native apps in cloud. In some competitive spaces, FIs may compete with cloud-native fintechs or BigTechs, who may not be licensed as FIs. For definitions of **"public cloud"** and other key terms, see **Annex 1** – Glossary.

---

[1] We interviewed central banks, bank supervisors, securities regulators and monetary authorities across Australia, Hong Kong SAR, India, Indonesia, Japan, Malaysia, Philippines, Singapore, Thailand and Vietnam. Those authorities are named in the acknowledgements on p. 2. Figures throughout the report are shown as a percentage of all agencies that responded to the particular question.

[2] See IIF, Cloud Computing in the Financial Sector Part 1: An Essential Enabler (Aug 2018); Part 2 Cloud Computing in the Financial Sector Part 2: Barriers to Adoption (Oct 2018); Part 3: Cloud Computing in the Financial Sector Part 3: Cloud Service Providers (February 2019); Cloud Computing: A Vital Enabler in Times of Disruption (June 2020).

[3] IIF – Deloitte, Realizing the Digital Promise series: Part 1 The Top Nine Challenges to Digital Transformation for Financial Institutions (February 2020); Part 2 Key Enablers for Digital Transformation in Financial Services (June 2020); Realizing the digital promise: COVID-19 catalyzes and accelerates transformation (June 2020); Part 3 Transformation in an ecosystem of regulators (April 2021); and Realizing the Digital Promise: Call to Action (October 2021).

2 Background

Cloud adoption globally and across sectors is expanding rapidly and very high growth rates are observed, particularly in Asia-Pacific. Financial services are no exception to this overall trend; cloud adoption in financial services is increasing and there is an increasing diversity and variety of use cases, deployment models and service types being used by FIs. Cloud is increasingly an enabler of the digital transformation of FIs as well as cyber resilience and financial inclusion.

2.1 Current trends

2.1.1 Cloud adoption growth rates

Cloud computing is experiencing rapid growth in revenues across industry sectors generally. The global cloud computing market size is expected to grow from $445.3 billion[4] in 2021 to $947.3 billion by 2026, at a Compound Annual Growth Rate (**CAGR**) of 16.3% during the forecast period.[5] The global cloud storage market is projected to grow from $76.43 billion in 2021 to $390.33 billion in 2028 at a CAGR of 26.2% during the forecast period.[6] By 2025, it is estimated there will be over 100 zettabytes (i.e., 100 trillion gigabytes) of data stored in the cloud.[7]

Growth rates in Asia-Pacific for cloud services are even higher. The biggest market in the Asia-Pacific region, China's total cloud infrastructure spending grew to $19 billion in 2020, a 66% annual increase.[8] Although the cloud market's total size in South-East Asia is still relatively small, it grew by more than 50% in 2020.[9] IDC estimated that in Asia-Pacific excluding Japan (**APEJ**), public cloud spending of financial services institutions was set to grow more than three times from $4.9 billion in 2019 to $18.1 billion in 2024 at a CAGR of 29.9%.[10]

2.1.2 Cloud in financial services

In 2019, the Financial Stability Board (FSB) reported that the deployment of cloud technologies in the financial service industry is still at its initial phase, with around 70% of financial services companies reporting at that time that they were only at the initial or trial and testing stage.[11]

Somewhat by contrast, a Harris poll surveyed risk/compliance and IT leaders in the banking and financial services industry across North America, Europe and Asia-Pacific worldwide in December 2020 and January 2021. The survey found that 83% of respondents in these regions are already using some form of public cloud, including hybrid and multi-cloud approaches. Many core financial workloads, however, remained on-premises, presenting an opportunity for these institutions to innovate further via the cloud. Additionally, those who currently use an on-

---

[4] All monetary amounts quoted are denominated in USD.

[5] Markets and Markets (2021), Cloud Computing Market Size, Share and Global Market Forecast to 2026

[6] Fortune Business Insights (May 2021), Cloud Storage Market Size, Share & COVID-19 Impact Analysis

[7] Arcserve (2020), The 2020 Data Attack Surface Report

[8] Canalys (2021), Record breaking spend grows 62% in Q4 2020 to US$5.8 billion, 24 March

[9] The Economist (2021), "Chinese cloud giants eye South-East Asia", "18 August

[10] IDC (2021), Worldwide Public Cloud Services Spending Guide (January), as reported in Business Chief (2021), Trends shaping future of cloud in financial services APAC, 24 April

[11] Financial Stability Board (2019), Third-party dependencies in cloud services Considerations on financial stability implications, 9 December, p. 7.

premises strategy said their organizations planned to switch, on average, 40% of their business workloads to public cloud in the following 12 months. Of the organizations whose primary IT infrastructure is cloud-based, the highest levels of cloud workload adoption were reported in North America, with the United States leading at 54% and Canada at 52%, and the lowest levels of adoption in Japan at 42% among the ten economies studied. Of firms relying on a majority cloud strategy, only about half (47%) of the firms' workloads were fully deployed to the cloud, with "core underwriting activity" ranking lowest in terms of full adoption.[12]

2.1.3 Increasing diversity of service types, deployment models and use cases in financial services

Recently, cloud in financial services has been characterised by an increasing diversity of service models, deployment types and use cases, and this trend is seen in Asia-Pacific as well.

As for service models, they continue to diversify and specialise. Traditionally private and public cloud offerings have been classified into Infrastructure as a Service (**IaaS**), Platform as a Service (**PaaS**) and Software as a Service (**SaaS**).[13] More recently, other more specialized service models observed include application PaaS (aPaaS), functions as a service (FaaS), database PaaS (dbPaaS), and application developer PaaS (adPaaS).[14]

IIF members are increasingly offering Banking as a Service (**BaaS**) in region to competitors and downstream FIs/fintechs. For example, Standard Chartered Bank's (**SCB's**) SC Ventures has launched its BaaS service nexus, signing Bukalapak and Socciola in Indonesia among other examples.[15] Ping An Group's One Connect also offers "technology as a service" to other FIs in Asia. Some other players exploring the BaaS model in Europe include solarisBank, Starling Bank and Fidor Bank.[16]

As for deployment models, beyond the usual trichotomy of on-premises, private cloud, and public cloud, other models have become evident such as virtual private cloud, hybrid cloud (the same FI adopting two or more of these three models) and so-called "community cloud" (whereby a CSP markets its offering as targeted at, and/or limited to, FI clients or the financial community).

Hybrid models in particular are expected to grow in importance: according to IDC, by 2023, 85% of tier-1 and tier-2 APEJ banks are expected to "curate" an infrastructure strategy by coalescing on-premises/dedicated private clouds and multiple public clouds, along with legacy platforms, to meet their infrastructure requirements. According to IDC, "Hybrid cloud environments and the use of multi-clouds mean a more agnostic experience for delivering container-based

---

[12] Google, Inc (2021), The Financial Services Industry Sees Increasing Public Cloud Adoption as Driving Innovation and Compliance, p. 3, 5, 11, 10.

[13] IaaS provides processing, storage and network services in a virtual environment. PaaS allows clients to develop and manage applications without building or maintaining any infrastructure and provides an application development and deployment environment in the cloud by offering the capability of utilizing computer programming languages and tools available from the service provider. Finally, SaaS provides a service that is offered directly to individuals or enterprises: see IIF (2018), Cloud Computing in the Financial Sector Part 1: An Essential Enabler, August, p. 2.

[14] BMC (2020), The 2020 Gartner Magic Quadrant for Cloud Infrastructure and Platform Services, 17 September.

[15] Crowdfundinsider.com (2021), New Digital Banking Services to be Offered by Standard Chartered and Indonesia's Bukalapak via the Nexus Platform, 15 January; IBS Intelligence (2020), nexus by Standard Chartered partners with Sociolla in Indonesia, 1 October.

[16] The Asian Banker (2020), StanChart's 'banking as a service' enables ecosystem players to offer financial services seamlessly, 5 May. IIF, Cloud Computing in the Financial Sector Part 1: An Essential Enabler (Aug 2018), p. 2.

workloads. Expanding microservices will offer increased tangible benefits and leverage developer independence, scalability, and rapid deployment capabilities."[17]

As for use cases, the Asia Cloud Computing Association (**ACCA**) has reported that since 2018, traditional FIs have accelerated their adoption of cloud as they transform their businesses through new customer offerings and advanced back office digitalization.[18] Financial use cases for cloud cited often include customer relationship management platforms (CRM), data analytics, fraud and risk, collaboration tools, infrastructure utilities, and enterprise services.[19] Typical use cases for cloud in financial services range from regulatory technology (**RegTech**) solutions such as anti-fraud and AML services that often make use of artificial intelligence (**AI**) and machine learning models, to rapid development of customer-facing apps which typically takes place in a cloud enabled development environment. It is also reported that supervisors have been exploring use cases for cloud computing in their own adoption of Supervisory Technology (**SupTech**).[20]

2.2 Cloud as an enabler of financial inclusion

Previous work has highlighted the potential for cloud adoption to increase financial inclusion. In a 2020 survey of official sector representatives focused on Asia-Pacific, more than 90% of respondents considered that innovations in digital payments processes were among the most significant areas in which fintech was improving financial inclusion objectives within their own jurisdiction.[21] According to 80% of survey respondents, the cost savings of information technology (**IT**) investment and the resultant increase in market competition were the primary benefits of cloud services to financial inclusion.[22]

Respondents also emphasised the cardinal role of digital identity and know-your-customer mechanisms in scaling up a secure digital financial system, with 69% of central banks in developing Asia selecting this as an essential feature to increase financial inclusion.[23]

Payments, including remittances, are a particularly relevant source of use cases for cloud gaining in prominence in Asia-Pacific. Remittance flows present a promising use case for cloud technologies to reduce costs and promote interoperability across different payment rails.[24] Many "paytechs" including names active in Asia-Pacific such as Wise, Revolut and NIUM are of course entirely or largely cloud native.

Microfinance is another sector where cloud is enabling financial inclusion goals to be met. For example, KreditBee's goal is to make it seamless for its target segment to gain access to different

---

[17] IDC (2021), Cloud Outlook 2021: Cloud Is Increasingly Becoming a Primary Route for Financial Services Collaboration, Innovation, and Transformation, March (subscription required for complete report).

[18] ACCA (2021), Better on the Cloud - Financial Services in Asia Pacific, 25 June, p. 13

[19] AFME - Protiviti (2021), Building Resilience in the Cloud, September, p. 7

[20] Financial Stability Institute (2018), Innovative technology in financial supervision (suptech): The experience of early users, July, p. 5

[21] Digital Monetary Institute (DMI) and AWS Institute (2020), Enabling financial inclusion in APAC through the Cloud (25 November), p. 7. In writing this report, the team surveyed and consulted 18 policy-makers, regulators and officials from central banks, supervisory authorities and international organizations. Of these institutions, 16 were from East, South and Southeast Asia.

[22] Ibid.

[23] Ibid.

[24] Id, p. 19

types of microloans, valued up to about $2,500, to pay for medical expenses, university tuition, or even online shopping.[25]

2.3 Cloud as an enabler of digital transformation and collaboration

The IIF has consistently emphasized the increasingly vital role of cloud as an enabler of digital transformation for FIs, as well as the contribution cloud has made to the resilience of FIs during the Covid-19 pandemic. These messages have come through in our own solo work on cloud and our joint work with Deloitte on digital transformation.

Cloud adoption enables incumbent FIs to modernize their core systems and technologies, to enable them to meet dramatically increasing customer expectations around the user experience (**UX**) and a generally more competitive landscape around new apps and services. In many cases those expectations have been raised by users' experience of the ease and convenience of BigTech applications including social media, digital wallets, and the like.

Cloud presents numerous benefits and opportunities in meeting evolving customer expectations. With greater customer demands for immediacy and personalization, as well as the increasing technical risk and cost associated with maintaining legacy IT infrastructure, the business case for adopting cloud technology is increasingly compelling, and the prevailing questions are less about "if," and more about "how."[26]

Cloud adoption also enables neobanks, insurtechs and fintechs/paytechs to build scale rapidly beyond initial deployment. As well, fintechs and other entrepreneurs can rapidly build and develop new applications, capitalizing on increased access to user data arising from open banking or consumer data right legal frameworks, or on contractual relationships with FIs through B2B partnerships.

It is well-known that the Covid-19 pandemic has seen a dramatic acceleration of digitalization in finance, including in volumes of digital payments and in eCommerce.[27] These trends have been observed strongly in Asia-Pacific. With this acceleration of digitalization, customers' expectations have risen around the speed and convenience of interactions, building on their experiences with BigTech in other sectors of their lives, such as entertainment, communications, eCommerce, online learning, and working from home. Digital transformation is no longer only about efficiency but has morphed to encompass business model transformation as customer expectations are unlikely to ever return to pre-pandemic dynamics.[28]

Increasingly, client interactions with FIs are mediated by platforms, typically cloud-enabled, that offer them access to products from more than one FI.[29] Another, related trend is the burgeoning use of cloud marketplaces speeding up collaboration between FIs and fintechs.[30]

---

[25] AWS (2021), KreditBee Tackles Financial Inclusion by Running Its Digital Lending Platform On AWS

[26] IIF (2018), Cloud Computing in the Financial Sector Part 2: Barriers to Adoption, October, p. 1

[27] E.g. YouGov (2020), How has the coronavirus pandemic impacted the use of cash globally?, November.

[28] IIF – Deloitte (2021), Realizing the Digital Promise: Call to Action, October, p. 2

[29] For a recent discussion of platforms in finance see Arner, Douglas W. et al. (2021) BigTech and Platform Finance: Governing FinTech 4.0 for Sustainable Development, 1 September.

[30] IDC (2021), Cloud Outlook 2021: Cloud Is Increasingly Becoming a Primary Route for Financial Services Collaboration, Innovation, and Transformation, March (subscription required for complete report).

3 FIs' perspectives on cloud adoption and regulation

To gather FIs' perspectives on cloud adoption and regulation we spoke to IIF member FIs active in the Asia-Pacific region, at up to Chief Digital Officer / Chief Information Officer (**CIO**) / Chief Operating Officer (**COO**) / Chief Data Scientist level. This helped to supplement and regionalize our own previous research on cloud and our joint work with Deloitte on digital transformation, where cloud has featured strongly as a foundational technology. We also hosted a session on cloud as part of the IIF's 2021 Annual Membership Meeting (**AMM**).[31]

3.1 The cloud adoption journey

3.1.1 Cloud adoption as an enabler of digital transformation and resilience

Generally, IIF members consulted are enthusiastic about the abilities of the cloud, and public cloud in particular, in both enabling digital transformation and in helping FIs to meet the challenges of increasing competition and user expectations, especially around UX.

> *Cloud is definitely an enabler, it's critical to the ability to develop new propositions to react to market developments.* ***– Chief Data Scientist, globally active regional bank.***

Typically, digital-only "neobanks" or "insurtechs" such as those that have been licensed recently in Singapore and Hong Kong are cloud-native; in these cases all their functionalities can be considered examples of use cases for cloud in financial services. One example is Mox Bank, one of the fastest-growing banks in Hong Kong history, which went from initial licensing to market deployment of its cloud-native and digital bank in 18 months. Developed as a joint venture, the cloud-native and mobile-only digital bank brings together SCB with telecom and lifestyle player HKT and other partners.[32]

The link with enterprise-wide business transformation was made explicit by one CIO:

> *We don't look at [cloud] as a "technology thing". It is enterprise-wide transformation. Roles are changing. Businesses need to think differently – from processes to people. … Cloud helps us do a hundred concurrent projects. You can perform cheaper innovation because you can test more easily.* ***– CIO, regional bank***

The IIF's previous work has emphasised the value of cloud as an enabler of resilience throughout the Covid-19 pandemic, as shown in the massive and largely seamless shift to working from home and remote servicing that it has enabled, and as a product of its distributed, redundant and scalable nature.[33] Reflecting this, one regional COO spoke of the contribution of cloud to pandemic resilience through the use of remote onboarding and verification tools:

> *Until 18 months ago, it was commodity data storage and compute services that cloud offered; during the pandemic cloud has been key to eliminating wet signatures and face to face selling.* ***– Regional COO, global insurer***

---

[31] Video available at the event's landing p. at https://portal.iif.com/Events/Meeting-Home-P.?meetingid={42B0D4E3-2866-EB11-80EB-000D3A0EE4ED} (IIF logon required).

[32] See AWS (2020), Mox Bank, GFT, & Thought Machine, December.

[33] IIF (2020), Cloud Computing: A Vital Enabler in Times of Disruption, June.

3.1.2 Cost savings

In a study across industries, Deloitte reported an average net return of up to $2.5 for every $1 invested in cloud services, notably through an average reduction of 19% in IT capital expenditure and an average staff time savings of two to three hours per employee per week.[34]

Consistently with this, generally, we found that FIs expect to reap considerable savings from cloud adoption. For example, one regional bank CIO overseeing a cloud migration program quoted previous experience in another sector as leading him to expect a close to 40% drop in overall costs over a five-year period. Some FIs also mentioned they value the ability to effectively recharacterize what would otherwise be significant capex as opex.[35]

Speaking at the IIF's 2021 AMM, Standard Bank Group's Head, Enterprise Data Office, John Linfield linked cost savings to scalability of cloud services:

> *One of the key benefits within cloud is in its scalability, and the fact that you can scale it according to specific workloads. […] Provisioning on premise infrastructure to multiples of average use is expensive, whereas cloud starts to give you the option that you can pay for this extra processing power when required, and really only when required.*

3.1.3 Governance and organizational change

While FIs perceive many actual and potential benefits from cloud adoption, they are also focused on identifying and addressing the challenges that are met as part of the "cloud adoption journey".

Many FIs report having cloud migration roadmaps or plans in place governing the migration process, typically with a 3 – 5 years' time horizon. In some cases, the end point is total migration of all services, but more often the FI's plans are subject to review, and migration begins with the more peripheral services, or with deployment of new cloud-based apps, services and subsidiaries.

Board level buy-in is seen as crucial to adopting and implementing a successful cloud adoption strategy. In the case of a global bank, the cloud migration plan requires global board support.

> *"Innovate or die." Our Board understands that. Our virtual bank is based on cloud. That is the level of focus and investment that can't be done without Board buy-in. –* ***Regulatory and Technology Strategist, global bank***

3.1.4 Talent acquisition and retention

We heard a variety of views from FIs on talent availability.

---

[34] FSB (2019), Third-party dependencies in cloud services: Considerations on financial stability implications, 19 December.

[35] See also FINRA (2021), Cloud Computing in the Securities Industry, at p. 2 and FSB (2019) *op. cit.*,), at p. 24-26. See also the discussion in section 4.2 for the authorities' perspectives on the cost issue.

One regional bank's CIO told us there was a talent shortage in their home country, but there was a difference between theoretical and real-life experience; talent with the right skills was in high demand. At our 2021 AMM, one speaker summarized the difficulty of attracting and retaining talent with the right digital skills:

> *I've never seen the war for talent to be as intense as it is right now Every industry is going after the same skill set. Every industry is transforming digitally in one way or another and so we are now not only competing amongst ourselves with other FIs, but we are competing across industries.* ***– Rizwan Khalfan, Chief Digital and Payments Officer, TD Bank Group***

By contrast, the Chief Data Scientist of a globally active regional bank said the talent issue is gradually easing, and that there are a lot more engineers available including many who understand data and the cloud.[36]

3.1.5 Managing complexity

Incumbent FIs with complex legacy systems and data architectures can find it a challenge to migrate to the cloud. As one interviewee said:

> *The difference between "lift and shift" to the cloud vs optimising to get better usage and value from data can be overlooked. Data scientists need appropriate data management skills, to ensure that data structures and models are not lost when data is placed in the cloud.* ***– Chief Data Scientist, globally active regional bank***

In this person's view, the appropriate skills are needed, also to address the possible improvement in data structures that can be affected.

Challenges related to the legacy environment of traditional FIs and their migration to the cloud were also addressed at the IIF's 2021 AMM:

> *Multinational organizations with a long history are likely to have a broad mix of technologies with a complicated set of integrations between those that have been built up over many, many years. Trying to transition those systems into the cloud as is risks simply migrating this complexity into a new environment and so we want to ensure that the transition is managed in conjunction with a program to simplify that legacy environment and to try and ensure that best practices, particularly around privacy and data management, can be achieved at the time of transition.* ***– John Linfield, Head, Enterprise Data Office, Standard Bank Group***

3.2 Regulation as an enabler and as a barrier to cloud adoption

3.2.1 Can supervisors act as an enabler of cloud adoption?

Some of the FIs we engaged with agreed that the supervisor has a big part to play in enabling FIs to adopt cloud.

> *We have cadence meetings with the regulator – every month we tell them what we want to move to the cloud so they see it in advance. … When we maintain that cadence*

[36] See the discussion in section 4.3 below for the authorities' perspectives on the talent issue.

we get into a flow. We involve them and this has helped the relationship and for us to move quicker and innovate. ***– CIO, regional bank***

In section 4, we will discuss further the supervisor's perspective including the different approval/notification processes deployed and what they learn from the pipeline of cloud projects.

3.2.2 Data localization requirements

FIs we asked about regulatory pain points tended to revert to the topic of data localization. These measures can take 3 broad forms:

- conditional limitations on data export (for example, on personal identifying information);[37]
- local copy requirements, i.e. the requirement to maintain a local copy of a particular data set in jurisdiction;
- "hard" localization, i.e. outright prohibitions on data export, or where export is only permitted under very challenging conditions (such as individual regulator approvals).

The FIs we engaged with said that data localization requirements, particularly the second and third types, can have several important negative effects:

- limiting the economies of scale that would otherwise be reaped from cloud solutions;
- increasing cyber risk by increasing the attack surface for cyber-attacks;
- reducing or eliminating the scope for data aggregation, and therefore limiting the ability to accurately model global risk and also the effectiveness of anti-fraud or AML systems.

We deal with these effects at greater length in our recent paper on a strategic framework for digital economic cooperation:

> *Beyond the direct costs within our industry, the impacts transmitted across the entire economy include weakened systems, reduced connections to global value chains, and less opportunity to leverage global data and technology resources in areas including fraud prevention and efficient payments.* [38]

From the IIF's perspective, fundamentally data localization interferes with the principle that data has greatest value when it is able to be utilized freely (with client consent). Data localization requirements that prevent the flow of data, or render that flow more expensive, therefore involve an impairment in value that would otherwise be present.

> *Data's value is maximized when it can flow with trust and permission across companies, sectors, and national borders to be used.*[39]

One particular frustration for regionally active FIs is those jurisdictions that provide for exceptions to data localization on paper, but where the process for activating those exceptions

---

[37] for example where personal identifying information may only be exported subject to appropriate relevant controls, or client confidential information may not be exported without client consent.

[38] IIF (2021), Strategic Framework for Digital Economic Cooperation, 12 October, p. 11.

[39] IIF (2020), Data Localization: Costs, Tradeoffs, and Impacts Across the Economy, December, pp. 2-3.

leads nowhere. In one example mentioned, in a regional economy[40] , an FI decided to pull an application after 18 months of inconclusive discussion with the local authorities.

Jurisdictions mentioned as having very stringent data localization rules include Indonesia, South Korea, Thailand (in respect of health data), and China, where there are overlapping requirements emanating from a number of different levels of government and different authorities. India was cited by one FI as having data localization rules that were subject to changing (and increasingly stringent) interpretations over time.

Data "siloing" can affect regionally active FIs in quite surprising ways. One FI remarked,

> *One key pain point is the mismatch between local copy requirements or data localisation requirements and the appetite of vendors to service those geographies. For example, the Office 365 suite is basic but an inability to deploy it in some countries leads to parts of the business being "islands".* ***– Regional COO, global insurer***

In terms of mitigants in the presence of data barriers and data silos, the Chief Data Scientist at one globally active regional bank referred to the possibility of federated learning, which uses privacy enhanced techniques to tune models across data boundaries. The Financial Conduct Authority (**FCA**) TechSprint conducted in 2019, which included aspects of federated learning, was cited as very helpful in this regard.[41]

[40] This regional economy is not one of the ten economies mentioned in the Acknowledgements on p. 2.

[41] See 2019 Global AML and Financial Crime TechSprint | FCA.

4 Authorities' attitudes to cloud in region

The following section summarizes the results of our engagement with authorities (central banks, monetary authorities, bank supervisors or securities regulators) in the region.[42]

4.1 Cloud adoption trends and developments

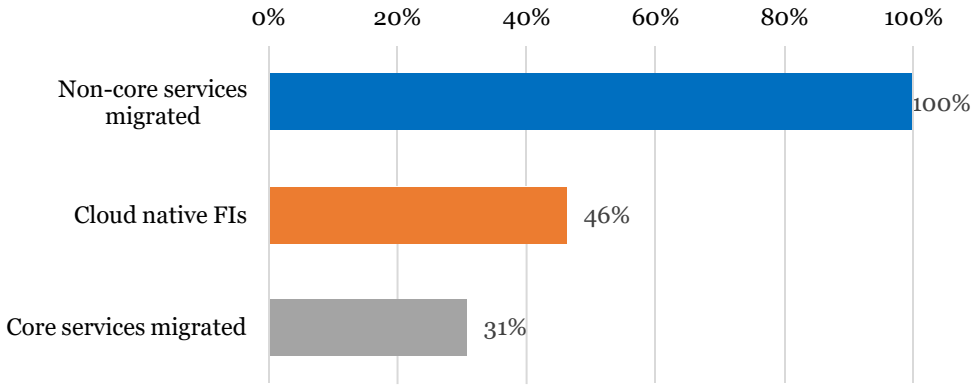
Authorities reported that levels of cloud adoption by FIs is increasing and, in many jurisdictions, accelerating. Regulators in key financial centers are seeing a steady rise in cloud adoption; particularly over the past three years, there has been a significant pick-up in adoption across the various service models (IaaS, PaaS, SaaS) and also across the public, private, and hybrid delivery models.

Several authorities are undertaking their own "cloud journey," deploying cloud for use in a variety of ways ranging from office systems and market supervision platforms to the provision of market infrastructure and common goods.

While few jurisdictions have yet seen large established FIs migrating core banking systems to the cloud, many FIs are deploying new applications to the cloud or migrating less-critical applications. Moreover, most holders of virtual or digital bank licenses, neobanks and insurtechs are cloud-native.

Somewhat consistently with this, authorities the IIF interviewed for this study reported observing a mixture of cloud adoption styles. All the authorities surveyed reported non-core services being migrated to the cloud by FIs in their jurisdiction. In around half of cases, those authorities also oversaw cloud-native FIs. In around a third of cases, authorities reported core services being migrated to the cloud, typically by smaller FIs (**Figure 1**).

Figure 1: Cloud adoption trends observed by authorities *
% of agencies



* Agencies were able to nominate as many trends as appropriate. Sample size of 13.

[42] Charts show the breakdown of answers given; in some cases authorities did not answer, or clearly answer, all aspects of our questions so in such cases the sample size is less than 15.

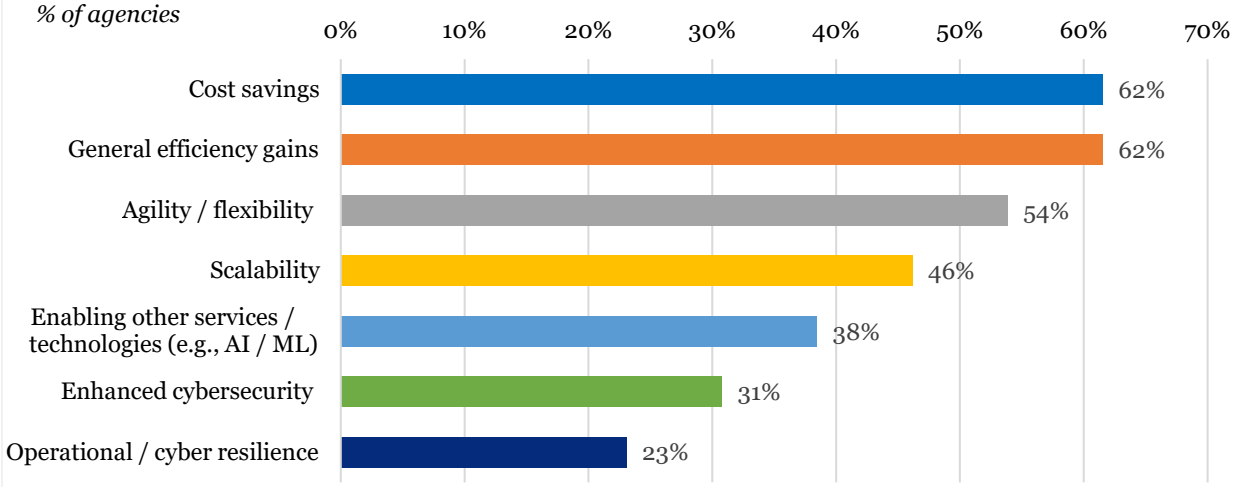
Typically, authorities interviewed reported that FIs in the economies in scope are served by the three largest US-based CSPs[43] and by CSPs based in Europe and Asia, some of which in turn outsource to the major US-based providers. CSPs have data centers in an increasing number of jurisdictions in region. China-based CSPs are not typically used at scale by FIs in countries outside China at present.

4.2 Benefits of cloud adoption

Cost savings, general efficiency gains, and agility/flexibility were each noted by a majority or near-majority of the authorities in our sample as some of the perceived benefits of cloud adoption, while over a third of respondents identified cloud's ability to enable other services or technologies such as AI and machine learning (**Figure 2**). One bank supervisor shared that the average savings obtained by respondent banks is estimated to be 39% of the total cost of procurement and maintenance of non-cloud computing IT.

Figure 2: What are the observed or perceived benefits from public cloud adoption? *

% of agencies



* Agencies were able to nominate as many benefits as appropriate. Sample of 13 agencies.

One monetary authority remarked, "Firms can 'spin up' services on the cloud as needed so managing that expenditure and resources is simpler for them." Another bank supervisor warned of the flip side, saying that cloud is not always cheaper than the alternatives; it is relatively easy to "spin up" new environments and each has a financial overhead that needs to be carefully managed by the customer.

One securities regulator interviewed mentioned that cost savings to date from their own cloud migration had been greater than expected as unit costs came down, while also mentioning benefits in terms of data governance, data hygiene, and potentially data sharing.

[43] i.e., Amazon Web Services, Google Cloud and Microsoft Azure.

4.3 Talent availability

Availability and retention of talent is an issue, particularly specific, granular expertise around cloud migration, data management, and the characteristics of particular CSP offerings. Of the 14 agencies that responded on this topic, 86% mentioned that there was a shortage to some degree of suitably qualified talent, at FIs or at their own agency, knowledgeable about cloud adoption.

In some jurisdictions this issue is perceived to be easing, while in others it is expected to emerge more strongly as cloud adoption grows.

Travel restrictions arising from the Covid-19 pandemic were not perceived by one authority as impacting talent availability greatly due to the ease of teleworking in this sector, while another stated that due to pandemic travel restrictions financial institutions—who in normal times tended to hire foreign nationals—were competing with it more to hire skilled staff.

Multi-cloud strategies, which may be adopted for reasons ranging from exit planning to deal with different service provisions in different countries, are seen as potentially exacerbating talent issues.

A number of regulators (and some FIs) mentioned they saw FIs reskilling existing workforces as essential in addressing this issue. Other mitigants mentioned by one authority for its own talent shortage included partnering with CSPs and consultants, along with reskilling existing on-premises team members.

One monetary authority goes further than regional peers in its efforts to foster talent:

> *We foster multiple schemes for practitioners to upskill, such as by inviting CSPs to give free training, and in future by working with universities to ensure that computer science courses are relevant to these new technologies.* – ***Monetary authority fintech head***

4.4 Regulation and supervision of FIs' cloud adoption

4.4.1 Regulation of cloud adoption

There is more commonality of approach than divergence across the region around cloud—regulators see it as a form of outsourcing, and all look squarely to the FI as the responsible entity.

All regulators are aware of the benefits of cloud, but most still see their role as ensuring that FIs manage the risk of cloud adoption, rather than emphasizing the risks of *not* adopting cloud. The link to digital transformation is less often drawn by supervisors.

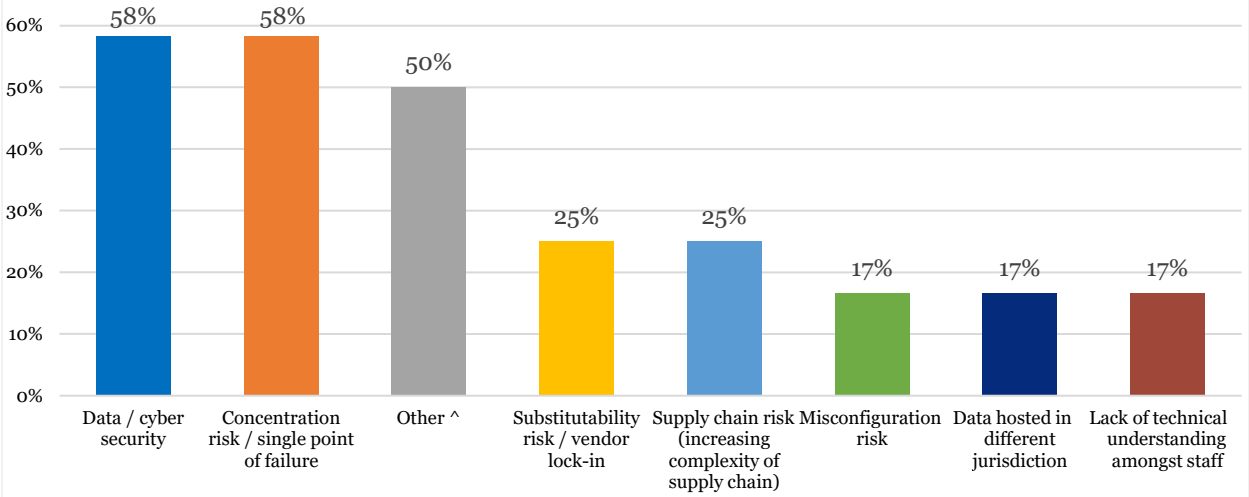
Risks to regulatory objectives are clearly defined and typically addressed through outsourcing and/or IT risk management guidelines, which have many commonalities, in many cases being based on relevant work of the Joint Forum, Basel Committee on Banking Supervision (**BCBS**) and/or International Organization of Securities Commissions (**IOSCO**).

Alongside outsourcing frameworks, many authorities publish cloud-specific guidelines as well, and many are considering updates. In the case of Singapore, the local banking association also provides industry guidance.[44]

Data/cyber security and concentration or single point of failure risk were the most frequently cited risks associated with public cloud adoption, with nearly six out of ten agencies mentioning each of these (**Figure 3**). Other risks mentioned included vendor lock-in, supply chain complexity, misconfiguration risk, and a variety of other risk categories.

Figure 3: What are the perceived risks to regulator objectives from public cloud adoption by FIs? *

% of agencies



*Agencies were able to nominate as many risks as appropriate. Sample size of 12 agencies.
^ For example, loss of direct control, inability to have complete transparency, lack of accountability, loss of governance, etc.

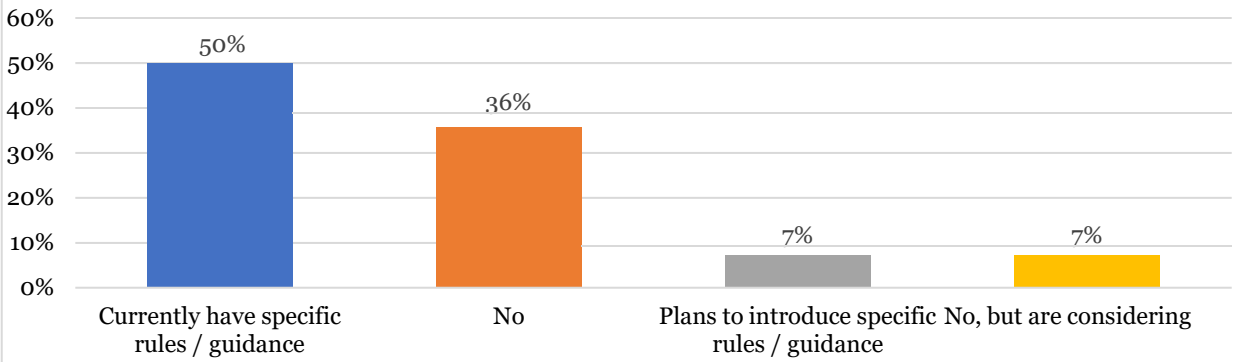
4.4.2 Cloud-specific guidance

Typically, regulators in the region see cloud adoption as a form of IT outsourcing and apply the risk management and cyber security policies that apply to the cloud adoption process.

Half of the respondent authorities indicated that they have cloud-specific rules/guidance for regulated entities, while 14% revealed they either already have plans to introduce such rules/guidance or are considering it (**Figure 4**).

[44] Association of Banks in Singapore (**ABS**) (2021) ABS Cloud Computing Implementation Guide 2.0 for the Financial Industry in Singapore, September

Figure 4: Does your agency have or plan to have cloud-specific rules / guidance for regulated entities? *
% of agencies



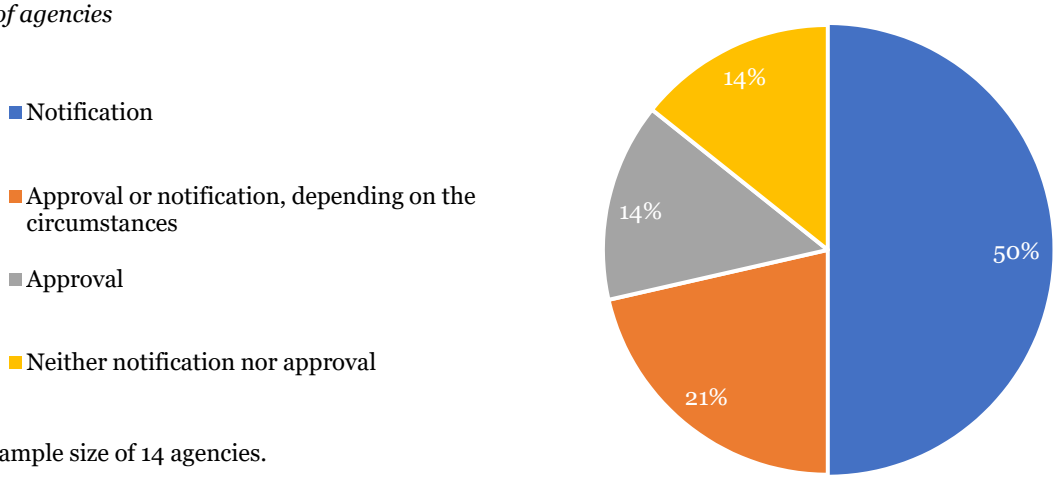
* Sample size of 14 agencies.

4.4.3 Notification and approval processes

Despite the commonalities, there are somewhat pronounced differences across the authorities in the region on whether notification to, or approval by, the supervisor of cloud adoption by supervised FIs is required and at what levels.

Half the responding authorities reported requiring notification in all cases, while around 1 in 7 reported having no notification or approval requirements, with the same number reporting always requiring approval; in the balance of cases (around 1 in 5) the authority's involvement varies according to circumstances, such as the type of cloud adoption—for example, outsourcing of core systems, or to certain types of premises (**Figure 5**).

Figure 5: Does FIs' public cloud adoption require notification or approval? *
% of agencies



* Sample size of 14 agencies.

While several authorities publish guidance notes and other frameworks that seek to define the categories of cloud adoption that require approval or notification, the Australian Prudential Regulation Authority (APRA) goes a step further and publishes a flowchart which provides FIs

with a graphical overview of the consultation and notification process relating to outsourcing involving cloud computing.[45]

4.5 Supervisors and CSPs

4.5.1 Nature and content of dialogue around cloud issues

We asked authorities about the nature of their dialogue with FIs regarding CSPs, with CSPs themselves, and with their peer regulators nationally and further afield.

A large majority (73%) of respondent authorities reported engaging bilaterally with FIs, CSPs, and with other domestic authorities around cloud. A further 9% reported bilateral engagement with FIs and CSPs, but not with other domestic authorities. Trilateral engagements with FIs and CSPs, which are typically limited to events, were reported by another 9% of respondents

Some of the modes in which authorities reported having domestic dialogue include:

- engaging directly with CSPs to gain a better understanding of the latest technical trends and service offerings to regulated FIs, their business and product strategies, the adoption of their services by local FIs, local support and infrastructure (including availability zones and underpinning data centres), and security capabilities;
- bilateral discussions with FIs and with CSPs, and also with financial or cloud industry associations, around new rules/frameworks and new guidance or FAQs, and pre-consultative meetings with licensees and prospective licensees, sometimes with a particular CSP they wish to use;
- discussions with other national financial regulators, in financial regulatory forums or bilaterally, on cloud-related topics.

In some jurisdictions, actual or proposed critical infrastructure legislation may apply to FIs and/or to some CSPs.[46] Several authorities reported dialogue with national critical infrastructure or cybersecurity authorities or centers; however, these discussions appear to be relatively nascent in region.

4.5.2 Direct vs indirect supervision

As is the case globally at present, CSPs are not directly regulated by financial supervisors in the region. Instead, central banks and supervisors exercise their oversight powers directly with regard to FIs, and only indirectly (if at all) with regard to CSPs themselves.

We also asked authorities for their views on the adequacy of the indirect model of supervision of CSPs, and about their monitoring of systemic risk.

Importantly, no regulators see the need at present to extend the perimeter of financial regulation to cover CSPs. They are cautious about the possibility and utility of extending it, given that

---

[45] APRA (2018), Information Paper: Outsourcing Involving Cloud Computing Services, 24 September, p. 24.

[46] For example, in Australia, legislation has been drafted, but has yet to be approved, that would directly impact CSPs if they are deemed 'systems of national significance'.

supervisors usually operate within a legal framework with a defined mandate, that CSPs service other sectors, and that they are sometimes based out of jurisdiction.

> *There may be a role for direct supervision of cloud service providers; however cloud providers are critical to a vast number of companies that do not provide financial services, and therefore sit outside our remit.* – ***Bank supervisor***

> *In practical terms, direct oversight would pose challenges given that the technical aspects of the major CSPs are operated outside our jurisdiction. Also, CSPs provide services to FIs and many non-financial entities, so it's not clear whether financial regulators are best placed to regulate CSPs.* – ***Securities regulator***

By the same token, the possibility of direct supervision at some point in the future was typically not ruled out, and some authorities were willing to mention possible models.

> *At the moment, we don't see the need to regulate CSPs directly. We have a handle on our regulated FIs, and we would expect them to manage [relevant] risks and if we thought that was insufficient we would obviously review and reconsider the situation.* – ***Securities regulator***

> *So far, the indirect supervision model has been sufficient, but we will keep international developments in view and formulate suitable measures if necessary.* – ***Monetary authority***

> *If we see [systemic risk] becomes critical in 5 to 10 years, we can start to think about the model we want and how to influence it.* – ***Monetary authority***

> *There are various possible models for future oversight arrangements, with the outcome defined as ensuring that we have confidence in the ability of CSPs to manage/mitigate risks appropriately. These models range from direct oversight to shared industry audits, to supervisory colleges, to a "financial sector cloud" model. We are keeping an open mind.* – ***Central bank***

4.6 Systemic risk levels, monitoring and mitigants

4.6.1 Perceived systemic risk levels

In terms of the overall level of systemic risk observed, no authorities judged that systemic risk concerns are critical or even, in some cases, material, given the existing levels of cloud adoption, so as to warrant regulatory action on their part. By the same token, most agencies responding indicated that they were closely watching for build-up of systemic risk.

> *To date we have not seen a need to materially intervene in the cloud marketplace either at the market dominance and related concentration risk, or at an entity vendor lock-in, level.* – ***Bank supervisor***

> *We do not have an immediate concern on concentration risk at this time and will monitor international developments, especially at FSB and IOSCO level, relating to operational resiliency and concentration.* – ***Securities regulator***

> *Based on the information gathered, we have not detected material systemic risk concentrations so far, although the use of cloud is on a rising trend, and we will*

*continue to monitor the situation closely and update our analyses regularly. – **Monetary authority***

*At present, the risk of systemic risk concentration is very low, as very few [local] FIs use core services on-cloud. – **Central bank***

On authority tied the level of systemic risk with the types of deployment model.

*To date, the adoption of cloud in financial services has been primarily in infrastructure (IaaS). This is increasingly becoming a commodity service, which can be provided by the different cloud service providers. The concentration and lock-in risks will increase with an increasing adoption platform as a service (PaaS) and Software as a Service (SaaS) models. – **Bank supervisor***

4.6.2 Systemic risk monitoring and mitigants

Many regulators have systems or personnel that seek to monitor systemic risk concentrations around cloud, either informally or through basic mapping of dependencies.

In several cases, a perhaps surprising degree of CSP-specific monitoring and risk mapping is undertaken within the indirect supervisory model.

*We are watching closely to see which public cloud is being used for what type of business systems, including core banking systems. – **Bank supervisor***

*Systemic risk is a risk that no individual FI can monitor on its own since they don't reliably have access to information about their competitors' arrangements. So the regulator must do systemic risk monitoring, we map dependencies of FIs to individual CSPs and individual availability zones within countries (including down to the data center level). – **Central bank***

*Our risk monitoring of individual CSPs includes dashboards that include how many institutions are with a particular CSP and for what solutions; when the last SOC-2 report was submitted; and open issues. In terms of systemic risk monitoring, relevant dimensions are the systemic importance of the FI and whether the outsourcing is of core or non-core systems. So far, we do not attempt to model the impact of a failure of one or more CSPs on the domestic financial system. We map inter-FI financial exposures, but not indirect exposures via shared CSPs. – **Central bank***

Apart from monitoring, a number of possible mitigants of systemic risk arising from cloud adoption, including from concentration in the market for CSPs, were mentioned by authorities, including business continuity planning (BCP) arrangements, exit plans, and multi-cloud.

*Taking into account how banks make use of availability zones, we focus on whether banks have adequate BCP processes to ensure continuity if there is disruption at the CSP level. – **Bank supervisor***

4.6.3 Global dependencies mapping

In a submission to the FSB dated 8 January 2021, the IIF suggested the possibility of global risk mapping around third-party dependencies, including cloud.[47] Some agencies agree there could be value in such global mapping of systemic risk concentrations, while one thought that broader cyber contagion risk mapping would be valuable, while a smaller economy central bank would prefer a regional to a global mapping exercise.

> *International cooperation could be worthwhile to take stock and identify interdependencies and potential systemic risks stemming from excessive concentration on one provider being used by multiple systemically important FMIs, or being used by different entities in the financial sector (e.g., FMIs and FIs).*
> ***– Central bank***

> *Global systemic risk monitoring around cloud would not be as useful as cyber contagion mapping at the national / global level mapping entire value chains (for example payments services) and identifying all key participants and their service providers. That would really hep supervision, more than CSP-specific risk mapping.*
> ***– Central bank***

> *Global work on interconnectedness of CSPs and FIs may be interesting but of limited value to a jurisdiction like ours, due to low materiality of local players globally. A regional attempt to map these interdependencies would be more helpful for us.*
> ***– Central bank***

4.7 International cooperation

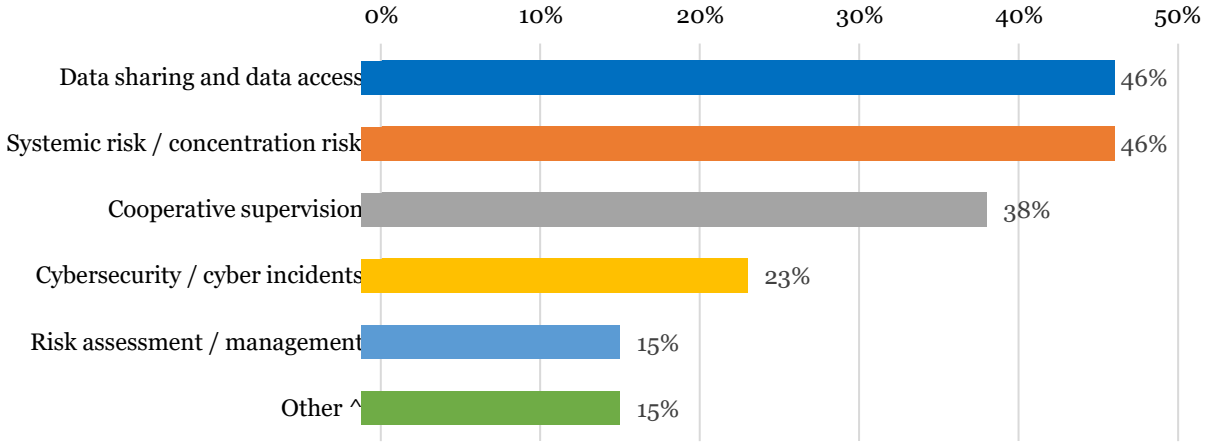
Central banks and supervisors in the region are active in FSB, BCBS and/or IOSCO discussions around cloud and outsourcing; for example, the ongoing FSB work on outsourcing and third-party risk management, and work at the Basel Committee on principles for operational resilience and at IOSCO on principles for outsourcing. Regional forums such as the Association of Southeast Asian Nations (ASEAN), Executives' Meeting of East Asia-Pacific Central Banks (EMEAP), the FSB Regional Consultative Group for Asia, and the Basel Consultative Group are also seen as important forums for information sharing and joint work on these issues.

When asked in what areas more international supervisory or regulatory coordination would be helpful, authorities highlighted data sharing/access, systemic risk/concentration risk, and cooperative supervision most frequently (see **Figure 6**). Additional issues mentioned include cybersecurity/cyber incidents, general risk assessment or management topics, and other issues such as potential constraints on supervisory access rights.

[47] IIF (2021), Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, 8 January.

Figure 6: On what topics would more international or regional harmonisation or supervisory cooperation around public cloud adoption be valuable? *

% of agencies



* Agencies were able to nominate as many topics as appropriate. Sample size of 13 agencies.
^ For example, substitutability, service continuity, auditing, and constraints on supervisory access rights.

4.8 Cyber security

4.8.1 Benefits and risks

Regulators generally see potential benefits, particularly for smaller institutions, in terms of cyber security from cloud adoption, given the increased sophistication of cyber defenses and patching at CSPs, as well as failover arrangements.

In terms of risks, many warn that misconfiguration risk is key and that FIs need to fully understand all aspects of cloud installations they are responsible for. One official explained how security controls that are inaccurately configured or left insecure can put a firm's systems and data at risk, so firms must be careful to avoid a false sense of security simply because they migrated to the cloud.

Another official highlighted how cybersecurity concerns are moving from an individual risk to a potential source of systemic risk with greater interconnection between technology and the financial system. He cautioned that FIs should ensure that the third party should have an effective IT and cyber security control in line with international standards and the FI's own security standards, and that the FI should also continuously conduct and monitor services operated by those external service providers.

4.8.2 Shared responsibility model

Under the "shared responsibility" model both the FI and the CSP take responsibility for activities, such as security and compliance, that are required for running a public cloud service. The CSP manages elements such as the provision of servers, networking, and data center facilities, whilst

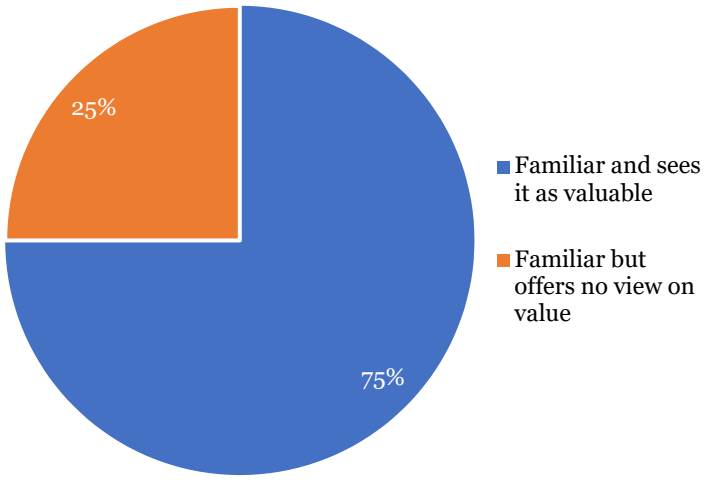
the FI is responsible for aspects such as customer data, security, application management, and user access. The FI maintains sole regulatory responsibility for the service.[48]

The shared responsibility model is typically seen by authorities as valuable, but as not overriding the FI's accountability to the regulator. All 12 of the agencies that responded on this topic indicated that they are familiar with the model, and three-quarters of those entities reported finding the model valuable (see **Figure 7**).

One official explained that while the shared responsibility model was valuable—for example for better customization of services—it is critical for FIs to have granular knowledge of their responsibilities for aspects of the overall security configuration. He went on to say that it is key for FIs to establish cloud governance frameworks and conduct sufficient assessment to identify and manage the relevant risks. Some authorities also drew a link between this issue and that of talent availability, given the need for sufficient expertise to be available to understand the range of tasks allocated to the client under the particular shared responsibility model in place under the relevant service agreement and to operate the appropriate governance arrangements.

Some acknowledged the availability of tools that CSPs provide to automatically identify configuration vulnerabilities.

Figure 7: Is your agency familiar with the so-called "shared responsibility" model? Do you see this model as valuable? *
% of agencies



* Sample size of 12 agencies.

[48] Asia Securities Industry & Financial Markets Association (Asifma) (2021), Proposed Asifma principles for public cloud regulation, March, p. 5.

4.9 Data localization

There is a variety of attitudes to whether data relating to FIs or their clients should be held locally (either in local copy or by prohibiting export), but all jurisdictions insist on ready regulatory access to data held in the cloud as being key.

> *The key consideration remains that we must have unfettered access to bank data required for discharging its regulatory function. The same principle applies to cloud outsourcing, which is a type of technology outsourcing. We believe our focus on supervisory access does not, and would not, cause barriers for technology adoption, including cloud adoption.* – ***Monetary authority***

Jurisdictions with data localization rules cite a wide variety of regulatory objectives, for example protecting national security, protecting individual privacy, securing ready access to data for law enforcement or for supervision or resolution authorities, increasing economic growth or employment or ensuring self-reliance, preventing foreign surveillance, enforcing data protection laws, and mitigating geopolitical risk from spilling-over to the domestic system.

Many jurisdictions make an exception from data localization rules for foreign-headquartered banks; however, as mentioned the experience of FIs can be that such exceptions can be difficult and time-consuming to try to utilize, without guarantee of success.[49]

Interestingly, one jurisdiction mentioned seeking to ensure that foreign regulators, law enforcement or security agencies cannot access data without permission by requiring that data is encrypted at the CSP, and that encryption keys remain local, even if data is held remotely. This appears to the IIF to be a pragmatic and desirable "half-way house" that delivers the regulator one regulatory objective (i.e., preventing unauthorized foreign access, and having a means of data access in the jurisdiction) without requiring that the actual data be held locally.

4.10 Audit and outsourcing

Regulators typically do not require adherence to specific standards in their guidelines (such as ISO, NIST or other standards), but assume that such standards will exist and continue to evolve and inform both CSP self-certifications and external assurance. The Bank of Japan has published a useful chart cross-referencing the applicable ISO, NIST, FISC, and ISMAP standards.[50]

Many regulators expect that FIs will insert specific clauses or protocols in contracts with CSPs to preserve their own, or their regulators', access to data, or to premises, to support audit or oversight rights.

> *Internal Audit will almost always need to rely on third-party assurance for the controls managed by the CSP. Despite this, there is still a highly important role for Internal Audit, to directly assess the 'customer owned' controls under the shared responsibility model. At a bare minimum, this would include access rights to data and administration consoles. … The reality is that for practical reasons, Internal Audit's role when an entity uses cloud services is still maturing.* – **Bank supervisor**

---

[49] See section 3.2.2.

[50] Bank of Japan (2021), Key Considerations for Risk Management in Using Cloud Services, Appendix on Necessary Management Items and Case Studies on Using Cloud Services, March.

The audits and certifications that CSPs are using do not necessarily cover all of the financial supervisory guidelines and industry guidelines. For this reason, it is reasonable for financial institutions to request audit firms that are well versed in cloud services in the financial sector for audits, as needed, in order to identify and control risks in a more detailed manner. **– Bank supervisor**

FIs should include the rights of the financial institution, internal auditors, external auditors, and the central bank to request relevant information and to examine the operation and internal control of the service provider, for both domestic and overseas service providers in the cloud computing agreements for critical systems. **– Central bank**

5 Recommendations

As stated in Section 1, in the IIF's view, the business risks to FIs of not adopting cloud are greater than the risks posed by cloud, due also to the competitive threat to regulated FIs from less regulated, and cloud-enabled, BigTechs and fintechs, in an environment of heightened user expectations, reduced margins and, for the present, cheap capital.

FIs and regulators therefore need to adopt approaches that help smooth cloud adoption, while always ensuring that risks are adequately monitored and managed.

The IIF's submission to the FSB dated 8 January 2021 on outsourcing and third party service providers (**TPSPs**) contains a number of recommendations for policymakers that may resonate in the Asia-Pacific region as well as globally.[51] The IIF and Deloitte have more recently jointly explored the challenges, barriers, and enablers of digital transformation for FIs, most recently through our "Call to Action" paper.[52] Cloud was identified in this report as a foundational technology, along with AI, and digital identity.

5.1 Key recommendations to authorities and stakeholders

The key recommendations made to the FSB and to authorities we have made are:

- Supervisors should adopt proportionate, risk-based, and outcomes-focused approaches to third-party arrangements, including with regard to materiality and criticality definitions.
- In order to improve alignment of terminology and concepts, we suggest an exercise similar to the FSB's cyber lexicon[53] which would standardize terminology largely by drawing on existing standard-setting bodies' (**SSBs'**) work, and which could be drawn upon in future standard-setting or regional/national rulemaking work.
- Regulators could facilitate joint industry audits or other collaborative reviews of TPSPs, to reduce the burden on FIs and TSPSs of duplicative information requests.
- Given that FIs themselves do not have visibility into the precise third-party arrangements that other FIs maintain, there may be a role for supervisors and global SSBs to map linkages between FIs and TPSPs, particularly where there is a high degree of concentration among them.
- Regulators should not dictate cloud models for FIs but should instead share the risk considerations they see and set risk standards for making deployment decisions.
- Regulators should work with cloud service providers and other vendors to ensure data portability and interoperability around the cloud.

---

[51] IIF (2021), Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, 8 January.

[52] IIF – Deloitte, Realizing the Digital Promise: Call to Action (October 12, 2021). The paper builds on the rest of the "Realizing the Digital Promise" series to date: Part 1 The Top Nine Challenges to Digital Transformation for Financial Institutions (February 19, 2020); Part 2 Key Enablers for Digital Transformation in Financial Services (June 4, 2020); Supplement COVID-19 Catalyzes and Accelerates Transformation in Financial Services (June 24, 2020); and Part 3 Transformation in an Ecosystem of Regulators, BigTech, FinTech and More (April 26, 2021).

[53] FSB (2018), Cyber Lexicon.

Our key recommendations to FIs and the broader stakeholder community (including regulators) arising from our work on cloud and digital transformation are:

- FIs should focus on developing an adoption plan based on their institution's strategic goals and objectives with risk management strategies. Regulators, meanwhile, need to work closely with FIs to enable safe and successful migration.
- Stakeholders need to work together to promote the safe, responsible, and successful adoption of key emerging technologies—including cloud, AI, and digital identity—as they are vital to supporting the next version of business models and to unlocking the full potential of the digital economy.
- More engagement between TPSPs, audit firms, audit standard-setters, financial regulators, and FIs could be helpful to clarify the content and nature of audits around specific topics such as cloud cyber security.
- Stakeholders should carefully consider the implications of establishing certifications of CSPs with direct supervisory oversight by financial service authorities.

5.2 Data localization

The recent IIF staff paper on digital economic cooperation[54] was sparked by industry leaders and public officials observing that we are fast approaching an inflection point and a "Digital Bretton Woods" may be needed to hammer out the new rules for a digital world. We aimed for the paper to provide a state of play outlining the problems and drawing attention to the potential harm that the global march towards a fragmented and isolated digital economic landscape could bring.

The next paper in this series will look at solutions to this problem both at a global level but also in nodes of likeminded markets who are tackling these issues in bilateral and multi-country trade and standards agreements. The digital transformation of financial services—with the adoption of cloud, AI/ML, and data solutions—presents an opportunity to update the policy frameworks that have shaped international policy coordination for the past several decades and help shape the larger process. These are complex and challenging problems with emotional national dynamics but if we don't find solutions the world risks a breakdown of the digital economy. No one will benefit from this outcome and the need for digital economic cooperation has never been greater.

As a guiding principle, regulators and policymakers are encouraged to be clear on the regulatory objective, demonstrate that the rules imposed are the least restrictive means of achieving those objectives, and remain open to new alternative solutions. Means such as encryption and other privacy-enhancing technologies should be explored, wherever practicable, as alternatives to rules that balkanize the global data economy and prevent the full value of data from being realized, to the ultimate benefit of clients and end users.

[54] IIF (2021), Strategic Framework for Digital Economic Cooperation (11 October).

6 Issues for further study

The IIF expects to engage with its members, with the official sector and with other actors, to work collaboratively on a range of topics that present themselves arising from the rise of cloud in financial services, in Asia-Pacific and beyond.

The key topics of discussion among the official sector, to which the IIF expects to contribute and, where appropriate, to help shape, are broadly speaking all focused on how to ensure that the efficiency, agility, cost, and financial inclusion benefits of cloud can be accessed widely, while ensuring that risks at the FI and systemic level are monitored and, where necessary, mitigated.

Some of the issues for further study include:

- appropriate monitoring arrangements with regard to CSPs, given that financial regulators do not typically have any direct regulatory relationship with them;
- defining and measuring systemic risk and concentration risk in the context of CSPs, and devising adequate mitigants for such risks that are not overly constraining and do not have unintended consequences;
- ensuring that regulators are transparent about the regulatory objectives sought to be achieved by measures such as data localization, and choose the least restrictive method of achieving those objectives;
- ensuring that CSPs are not subjected to duplicative or overly intrusive information requests by FIs, while ensuring that regulators have appropriate visibility into all relevant risks; and
- ensuring that FIs and their service providers including CSPs are not subject to unrealistic expectations that they are unable to fulfil, but at the same time fully understand their own responsibilities.

The IIF will look for opportunities to take this work forward in 2022 and beyond.

Annex 1: Glossary

AML: anti-money laundering.

AMM: 2021 IIF Annual Membership Meeting

BaaS or Banking as a Service: provision by a financial institution of a cloud-based banking solution enabling other "downstream" FIs to provide banking services without having to develop the core technologies used.

BigTechs: large social media and other technology firms.

CIO: Chief Information Officer.

COO: Chief Operating Officer.

Cloud: provision of information technology services by third-party service providers or outsourced service providers, typically under a contract with the client and typically involving remote data storage and processing of the client's own data.

Cloud adoption: migration of FI legacy systems/workloads to cloud; advent of totally cloud-native FIs and fintechs/techfins; and traditional FIs rolling out new cloud-native apps in cloud.

Community cloud: cloud offering whereby the CSP markets its offering as targeted at, and/or limited to, FI clients or the financial community.

CSP: cloud service provider.

Fintechs: financially-focused technology firms, providing services on a business-to-business (B2B) basis to financial institutions and/or on a business-to-client (B2C) basis

Hybrid cloud: services combining public and private cloud resources, with technology allowing data and applications to be shared between them.

IaaS or Infrastructure as a Service: model of cloud service where customers are supplied with IT infrastructure, provided and managed over the internet on a pay as you use basis, e.g., servers and storage.

Insurtechs: technology-focused or enabled insurance companies, or specialist B2B providers to insurance companies.

IT: information technology.

Neobanks: digital-only or branchless banks, either standalone entities or subsidiaries of traditional financial institutions.

On-premises or **on-prem**: IT installations held on the client's own premises, typically owned by the client.

Paytechs: fintechs active or specializing in the payments space.

Private cloud: services in which computing resources are used solely by one single organization, either physically in the company's on-site data center(s) ("on-premises") or externally with the third-party provider ("hosted private cloud").

Public cloud: services, including general computing and/or software resources, offered by a third-party provider over the public internet. Whilst these services are generally available to any entity willing to subscribe to them, access control functions ensure the proper usage of the services by the legitimate entity under a contractual agreement with the third-party provider.

PaaS or Platform as a Service: model of cloud service where customers are supplied with an on-demand environment for developing, testing, delivering, and managing software applications over the internet.

RegTech: regulatory technology, enabling FIs and others to comply with regulatory requirements, including reporting requirements.

SaaS or Software as a Service: model of cloud service allowing customers to connect to and use cloud-based applications over the Internet on a subscription basis.

SSB: standard-setting body.

SupTech: supervisory technology, enabling supervisors and central banks to monitor FIs' compliance with regulatory requirements or FIs' activities more broadly.

TPSP: third party service providers.

UX: user experience.

Annex 2: Questionnaire

Official sector agencies were engaged through oral or written interviews using the following questionnaire. In the case of one authority, the discussion was held in a free-form format on a variety of other topics.

1. **Preliminary**
   - In your agency's monitoring of public cloud adoption by FIs and/or SIFIs, what levels and trends have been observed?
   - What are your agency's observations on the availability of suitably qualified talent, at FIs or at your agency, knowledgeable about cloud adoption?
2. **Perceived benefits and risks of public cloud adoption for FIs**
   - What are the benefits from public cloud adoption by FIs your agency has seen or perceives would be possible? Notable instances of that in jurisdiction?
   - What are the perceived risks to regulatory objectives from public cloud adoption by FIs? How does your agency seek to manage those risks or have FIs manage those risks?
3. **Regulation and supervision of FIs**
   - Does FIs' public cloud adoption require notification or approval? If so, what needs to be notified/approved (program or workload) and which categories of FI are subject to the requirement (G-SIFI, D-SIFI, other, all)?
   - Does your agency have or plan to have public cloud-specific (or more broadly cloud-specific) rules or guidance for regulated entities? If yes, what are the key issues and concerns they address? How are your agency's regulatory objectives relevant?
4. **Regulation and CSPs**
   - What types of domestic dialogue/discussion does your agency engage in on public cloud issues (e.g., bilateral with FI; bilateral with CSPs; trilateral with FI and CSP; cross-sectoral)?
   - Until now, CSPs have not been regulated by FS regulators directly (and have been impacted by FIs' regulation only indirectly); is this considered as sufficient? Why or why not?
5. **Systemic risk monitoring and mitigants**
   - Having regard to the level of cloud adoption seen so far in your country, are there any concerns about systemic risk concentration arising from public cloud adoption? What if any mitigants or monitoring are in place or are under consideration relating to FI-specific or system-wide concentration risk?
6. **International cooperation**
   - On what topics would more international or regional harmonization or supervisory cooperation around public cloud adoption be valuable? What discussions is your agency involved in?
7. **Cybersecurity and data localization**
   - What are the key benefits or risks you are seeing around cybersecurity and public cloud? How are the benefits realized or the risks to be managed?
   - Is your agency familiar with the so-called "shared responsibility" model?[55] Do you see this model as valuable?

[55] Under the "shared responsibility" model both the FI and the CSP take responsibility for activities, such as security and compliance, that are required for running a public cloud service. The CSP manages elements such as the provision

- What data localization requirements (if any) does your agency impose on cloud adoption? If so, why are they adopted?

8. Audit and assessment of FIs' outsourcing to CSPs providing public cloud services

- In supervising FIs, which international standards for CSPs, or third-party certification schemes complied with or certified against by CSPs are recognized?
- Does regulator consider FIs' third-party ability to audit CSPs (under their contractual arrangements with CSPs) necessary given that CSPs already undergo compliance certifications and attestations by third-party, independent auditors? If yes, why and how should such audits be scoped to meet regulator needs?

of servers, networking, and data center facilities, whilst the FI is responsible for aspects such as customer data, security, application management, and user access. The FI maintains sole regulatory responsibility for the service. See Asifma (2021), Proposed Asifma principles for public cloud regulation, March. p. 5.

Annex 3: Bibliography

ACCA (2021), Better on the Cloud - Financial Services in Asia Pacific, 25 June

AFME - Protiviti (2021), Building Resilience in the Cloud, September

APRA (2018), Information Paper: Outsourcing Involving Cloud Computing Services, 24 September

Arcserve (2020), The 2020 Data Attack Surface Report

Arner, Douglas W. et al. (2021) BigTech and Platform Finance: Governing FinTech 4.0 for Sustainable Development, 1 September

Asia Securities Industry & Financial Markets Association (Asifma) (2021), Proposed Asifma principles for public cloud regulation, March

Association of Banks in Singapore (**ABS**) (2021) ABS Cloud Computing Implementation Guide 2.0 for the Financial Industry in Singapore, September

AWS (2020), Mox Bank, GFT, & Thought Machine, December

AWS (2021), KreditBee Tackles Financial Inclusion by Running Its Digital Lending Platform On AWS

Bank of Japan (2021), Key Considerations for Risk Management in Using Cloud Services, Appendix on Necessary Management Items and Case Studies on Using Cloud Services, March

BMC (2020), The 2020 Gartner Magic Quadrant for Cloud Infrastructure and Platform Services, 17 September

Canalys (2021), Record breaking spend grows 62% in Q4 2020 to US$5.8 billion, 24 March

Crowdfundinsider.com (2021), New Digital Banking Services to be Offered by Standard Chartered and Indonesia's Bukalapak via the Nexus Platform, January 15

Digital Monetary Institute and AWS Institute (2020), Enabling financial inclusion in APAC through the Cloud, 25 November

Financial Stability Board (2019), Third-party dependencies in cloud services Considerations on financial stability implications, 9 December

FINRA (2021), Cloud Computing in the Securities Industry

Financial Stability Institute (2018), Innovative technology in financial supervision (suptech): The experience of early users, July

Fortune Business Insights (2021), Cloud Storage Market Size, Share & COVID-19 Impact Analysis, May

FSB (2018), Cyber Lexicon, 12 November

FSB (2019), Third-party dependencies in cloud services: Considerations on financial stability implications, 19 December

FSB (2019), Third-party dependencies in cloud services: Considerations on financial stability implications, 19 December

Google, Inc (2021), The Financial Services Industry Sees Increasing Public Cloud Adoption as Driving Innovation and Compliance

IBS Intelligence (2020), nexus by Standard Chartered partners with Sociolla in Indonesia, 1 October

IDC (2021), Cloud Outlook 2021: Cloud Is Increasingly Becoming a Primary Route for Financial Services Collaboration, Innovation, and Transformation, March (subscription required for complete report)

IDC (2021), Cloud Outlook 2021: Cloud Is Increasingly Becoming a Primary Route for Financial Services Collaboration, Innovation, and Transformation, March (subscription required for complete report)

IDC (2021), Worldwide Public Cloud Services Spending Guide (January), as reported in Business Chief (2021), Trends shaping future of cloud in financial services APAC, 24 April

IIF (2018), Cloud Computing in the Financial Sector Part 1: An Essential Enabler, August

IIF (2018), Cloud Computing in the Financial Sector Part 2: Barriers to Adoption, October

IIF (2019), Cloud Computing in the Financial Sector Part 3: Cloud Service Providers, February

IIF (2020), Cloud Computing: A Vital Enabler in Times of Disruption, June

IIF (2020), Data Localization: Costs, Tradeoffs, and Impacts Across the Economy, December

IIF (2021), Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships, 8 January

IIF (2021), Strategic Framework for Digital Economic Cooperation, 11 October

IIF – Deloitte (2020), Realizing the Digital Promise series: Part 1 The Top Nine Challenges to Digital Transformation for Financial Institutions, February

IIF – Deloitte (2020), Part 2 Key Enablers for Digital Transformation in Financial Services, June

IIF – Deloitte (2020), Realizing the digital promise: COVID-19 catalyzes and accelerates transformation, June

IIF – Deloitte (2021), Part 3 Transformation in an ecosystem of regulators, April

IIF – Deloitte (2021), Realizing the Digital Promise: Call to Action, October 2021

Markets and Markets (2021), Cloud Computing Market Size, Share and Global Market Forecast to 2026

The Asian Banker (2020), StanChart's 'banking as a service' enables ecosystem players to offer financial services seamlessly, 5 May

The Economist (2021), Chinese cloud giants eye South-East Asia, 18 August

YouGov (2020), How has the coronavirus pandemic impacted the use of cash globally?, November

Authors

Laurence White
Head of Singapore Office Designate
Consultant – Asia Pacific, Digital Finance
lwhite@iif.com

Dennis Ferenzy
Associate Economist, Digital Finance
dferenzy@iif.com

Contributor

Conan French
Senior Advisor, Digital Finance
cfrench@iif.com