MILKEN INSTITUTE

FINANCIAL INNOVATIONS LAB®

Building Resilience: Cloud Adoption in Southeast Asia's Financial Sector

About the Milken Institute

The Milken Institute is a nonprofit, nonpartisan think tank. For the past three decades, the Milken Institute has served as a catalyst for practical, scalable solutions to global challenges by connecting human, financial, and educational resources to those who need them. Guided by a conviction that the best ideas, under-resourced, cannot succeed, we conduct research and analysis and convene top experts, innovators, and influencers from different backgrounds and competing viewpoints. We leverage this expertise and insight to construct programs and policy initiatives. These activities are designed to help people build meaningful lives in which they can experience health and well-being, pursue effective education and gainful employment, and access the resources required to create ever-expanding opportunities for themselves and their broader communities.

About the Financial Innovations Lab®

Financial Innovations Labs® bring together researchers, policymakers, and business, financial, and professional practitioners to create market-based solutions to business and public policy challenges. Using real and simulated case studies, participants consider and design alternative capital structures and then apply appropriate financial technologies to them.

About the Asia Center

The Milken Institute Asia Center extends the reach and impact of Milken Institute programs, events, and research to the Asia-Pacific region. We identify opportunities to leverage the Institute's global network to tackle regional challenges, as well as to integrate the region's perspectives into the development of solutions to persistent global challenges.

Acknowledgments

Jason Davis and Ella Tan prepared this report.

We are grateful to those who participated in the Financial Innovations Lab for their contributions to the ideas and recommendations summarized in this report. We would especially like to thank Google Cloud for its partnership on the project. We want to thank our Milken Institute colleagues Belinda Chng, Caitlin MacLean, Théo Cohan, and Cheryl Low for their work on the project. Finally, we would like to thank Editor Dinah Nichols for her work on the report.

CONTENTS

INTRODUCTION

The COVID-19 pandemic has made one thing clear: We will be living and working more on the cloud than we ever imagined. For firms worldwide that have operated for over a year under work-from-home mandates, country lockdowns, and volatile demand for products and services, the transition to a virtual office carries an added urgency beyond economic survival to designing for long-term corporate resilience and business continuity.

Fortunately for most firms, the digital shift had already begun with the widespread adoption of the internet for business use in the late 1990s and the subsequent steady digitization of tasks. In more recent years, cloud computing has become a massive part of global commerce, thanks to its capacity to strengthen security, store massive datasets, provide suites of software applications, and deliver analytics, networking, and other high-value services.

Banks and other financial institutions (FIs) have followed suit. A 2020 survey of US banks by the research firm Celent finds that "19 of the top 20 banks … [had] already announced public cloud initiatives," even as "fintech challenger banks and smaller financial institutions" were using the public cloud for core banking systems.[1] Before COVID-19, many banks and other FIs had announced plans to or had partly migrated to the cloud. In mid-2020, 95 percent of surveyed banks reported that they had already begun this transition, according to a report by Accenture. Still, most had only taken baby steps, and the clouds they referred to were their own private virtual networks, or VPNs.[2]

This scenario has also played out globally and in the 10 major countries of Southeast Asia. Banks have been slow to work with all the applications and functions fully and benefit from the ease of doing business that cloud computing offers. The individual institution and country reasons vary, but the region as a whole is confronting the uncertainty of a slow post-pandemic economic recovery.[3] The financial sector is strictly regulated, risk-averse, and reluctant to give up legacy IT infrastructure for a new business model. This stasis will work against them in a competitive global economy supercharged by financial technology.

In June 2021, the Milken Institute, in collaboration with Google Cloud, one of the largest cloud service providers (CSPs), hosted a virtual Financial Innovations Lab ("Lab") with a focus on the issues, both regional and local, for Southeast Asia financial institutions. Its purpose was to examine the region's challenges and identify potential avenues for a more timely and robust transition to cloud technology. The Lab brought together regional and international banking executives, technology experts, financial regulators, and multilateral organizations to develop recommendations. This summary distills the discussion and additional research, laying out potential paths forward in three critical areas of concern: regulatory compliance, data localization, and concentration risk.

ISSUES & PERSPECTIVES

State of Cloud Adoption by Financial Institutions

In 2009, a small FinTech firm in Amsterdam, Ohpen, created the first cloud-based core banking platform. Ohpen took on its first bank client three years later; today, the firm holds $92 billion in global assets under management. In the decade since Ohpen's debut, the overall global transition of banks and other FIs to the cloud has been steady but slow and cautious—and most have not migrated mission-critical core banking functions.[4]

This suggests that regulatory compliance is a major concern for financial institutions, and rightly so, as it can require conformity with industry, local, national, regional, and international security and privacy standards. Some anxieties were clearly set aside during the pandemic—banks had to contend with disruptions to their operations and those of their clients. In the US, for example, banks also found themselves on the frontlines, guiding small businesses and individuals through paycheck protection programs, debt relief and bridge loans, and mortgage and rent deferral plans, all through video calls, teleconferences, and other remote communications.

As a result of the "new normal" and uncertainties about the workplace of the future, banks have joined other businesses and gradually upgraded their systems to adopt cloud technologies. According to the global consulting firm Gartner, for firms globally, total business expenditures in public cloud computing services for 2021 are expected to reach $304.9 billion worldwide, up 18.4 percent from 2020. They also noted that "70% of organizations using cloud services today plan to increase their cloud spending in the wake of the disruption caused by COVID-19."[5] The sentiment is similar in the banking industry; Accenture reported that cloud investment for financial institutions worldwide was expected to increase by 15 percent by 2022 and hit $411 billion.[6] Total spending on public cloud services in the Asia/Pacific region (excluding Japan) grew in 2020 by 38 percent, or to $36.4 billion. The banking industry is expected to make up 10 percent of overall public cloud spending between 2021 and 2024.[7]

As more FIs go digital, they will have to consider how to maintain regulatory compliance within a complex regulatory landscape and harmonize compliance with regional and global rules. Both the institutions and their cloud service providers must also consider the impacts of the surge in national data localization laws that require citizens' cloud data to be processed, stored, and maintained in IT systems within the physical borders of their home country. And they must come to terms, for now at least, with the high concentration of US firms, and the growing number of Chinese

firms, among the quite limited number of cloud service providers. The Lab offers recommendations intended to alleviate concerns about all these issues.

Model and Service Options

The Lab began with a brief introduction to the major cloud deployment models and service categories.[8] Most businesses, including financial institutions, select from three cloud models: a public cloud, private cloud, or hybrid cloud.

In a **public cloud** environment, the CSP delivers services—whether storage, software, or platforms—by subscription and is responsible for management and upkeep of all related physical infrastructure (e.g., data centers and the servers, telecom, and other equipment they hold). The public cloud is widely understood to offer significant resilience and security benefits. The CSPs' servers and data centers in multiple locations make this model less vulnerable to disruption than a single business hosting data on its premises. The large CSPs also have the financial resources to make continual cybersecurity investments in "best-in-class protections."[9]

In **private cloud** computing, the institution may own its servers and the site for its housing. Its network is also private; employees access the cloud software and platform services either through the web or the company's virtual private network (VPN). In this way, the company has control over its data and privacy but must also maintains an IT department that manages the network, its security (firewalls), and related infrastructure upkeep.

Organizations can also opt for a **hybrid cloud** approach that benefits from combining a company's private cloud with the public cloud. The term "cloud" will refer to the public cloud in the rest of this document unless otherwise specified.

There are also three primary service options. Each comes with varying divisions of responsibility between the client firm and the CSP, and some may work better with one type of cloud model than another. Chart 1 illustrates these three primary service options.

Infrastructure as a Service (IaaS) allows customers to run their own operating systems and store their data on leased infrastructure, in the cloud or dedicated, eliminating the expense of firm-owned servers and data center and related equipment. Amazon Web Services, Microsoft Azure, Oracle Cloud Infrastructure, IBM Cloud, and Google Cloud are among the top IaaS providers.

Platform as a Service (PaaS) allows firms to use CSP hardware and software without investing in-house in the underlying technologies. The platform also offers application interfaces, code, and other development tools to enable a company to reduce the time to market for new applications. Major names in this arena again include Amazon Web Services, Google Cloud, Microsoft Azure, Heroku from Salesforce, IBM Cloud, and Oracle Cloud Infrastructure.

The most widely used cloud service model for businesses and individual users (e.g., Adobe, Gmail, or GoToMeeting) is ***Software as a Service*** (SaaS). This model provides ready-to-use software and application interfaces to clients when they log in, avoiding the need to install programs applications directly onto individual computers. Salesforce, Dropbox, and Google Workspace all offer SaaS.

CHART 1: CLOUD-BASED SERVICES DIVISION OF RESPONSIBILITY

On-Site Legacy IT Infrastructure	***Infrastructure as a Service (IaaS)***	***Platform as a Service (PaaS)***	***Software as a Service (SaaS)***
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

User manages Others manage

Source: BMC (2019), www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

BARRIERS TO ADOPTION AND INNOVATIVE SOLUTIONS

Lab participants discussed some of the most significant issues and challenges to full cloud adoption as cited by representatives of Southeast Asia's regulatory, technology, and financial sectors. These are laid out in more detail in the following sections, along with potential approaches toward solutions.

BARRIER: Regulatory Compliance

As noted, the public cloud is the most widely used deployment model worldwide, with new "community public clouds" offering a mix of public-private infrastructure ownership for industry-specific "community members" like financial institutions. The public cloud is known, among other benefits, for its cost-effectiveness (due to minimal capital outlay by subscribers), fast procurement of service, and instant global reach and interface. Nonetheless, the same concerns persist about the cloud and regulatory compliance, data integrity, and security. Responsibility for compliance and risk management lies ultimately with the financial institution that is the cloud service subscriber, often with the complication of regulatory ambiguity, not to mention differences across regulatory frameworks and jurisdictions. For example, unclear regulations in India often lead to FIs seeking regulatory approval to move each individual workload to the cloud, slowing down adoption considerably.[10] Of note, regulators are playing quick catch-up to the cloud and are working to tailor regulations to support cloud adoption. For example, the Bangko Sentral ng Pilipinas (Central Bank of Philippines) plans to release new outsourcing and IT management guidelines to allow banks to implement outsourcing arrangements without prior regulatory approval.[11]

Lab participants also expressed concern over designing audit rights that protect FI security, ensure transparency for auditors, and minimize the security risks that audits may cause the CSPs as third parties.

SOLUTION: Regional Standard for Data Classification

Data classification, in use for decades, is essential as a compliance and security tool. Companies, universities, and government agencies all use data classification to categorize, retrieve, track, and analyze their stored data. Organizations are then able to assign access and protection levels as well as security procedures. Classification also allows companies to separate data subject to regulation from that which is not.[12] For banks and other financial institutions holding vast troves of personal and financial information, proper data classification is the *sine qua non* of regulatory compliance.

No regional data classification standard is yet in place across Southeast Asia, though ASEAN recently launched the ASEAN Data Management Framework. It provides guidelines for organizing and classifying company data based on risk levels and ensuring appropriate risk controls are in place. The implementation of the framework is voluntary for businesses in ASEAN. Through the General Data Protection Regulation (GDPR), the European Union provides specific legal protections at a regional level for data that meets their definition of "personal data." Also, countries like the UK and US, which have well-developed domestic classification systems in place for their public data, will find it easier to fall into compliance with broader regulatory regimes.[13] Classification standards are beneficial as they serve as the basis for crucial downstream functions like data encryption, access requirements, and adherence to data localization laws. CSPs often help design data classification schemes and technical solutions for sorting structured and unstructured data. When datasets are categorized and labeled consistently, they merge properly, avoiding database errors.

A regional risk-based approach to data classification should consider current global industry models (e.g., the International Financial eXchange, or IFX, standard), a business message specification, and an interoperable standard for financial data exchange. Also of note is the Information FrameWork (IFW), a family of data, processes, and object models to help financial institutions transform cross-enterprise architectures. These existing models could serve as a harmonizing foundation for a new classification framework that regulators, a regional industry group, or other stakeholders could build out. In the US, the framework developed by the National Institute of Standards and Technology (NIST) is tiered according to risk assessment based on the impact a breach would have on the operations, assets, or individuals.[14] This kind of risk identification could be of great benefit to financial institutions.

SOLUTION: Regional CSP Certification Standard

As with regional classification standards, a regional CSP certification program brings long-term benefits. It can facilitate the FI cloud adoption process and aid regulatory compliance because it signals that the certified CSP meets common industry standards. This program would not substitute for due diligence; as noted, the individual organization bears the ultimate responsibility for its data integrity and security. But certification can help streamline the due diligence process, minimize related costs, and shorten adoption time.

Many certifications are already in effect, including those by the International Organization of Standardization (ISO) and the Payment Card Industry Data Security Standard (PCI DSS), and cover specific areas of commerce. Bringing these various certifications under a single certification can simplify the FI cloud adoption process. Still, it may be impossible to establish a single standard covering every aspect of the CSP/FI relationship. Participants suggested that until certification simplification emerges, compliance with a basket of existing, regionally accepted international standards could be effective. In the meantime, ASEAN is exploring a regional cross-jurisdictional certification system that employs current international standards and accredited third-party certification bodies. The organization is also exploring model contract clauses that FIs can use as they enter into agreements with CSPs, inspired by the European Union's Standard Contractual Clause. Notably, ASEAN's approach will incorporate a modular design to allow flexibility according to the type of data shared and data processing involved.

Enforcement is another challenge to regional certification. Stakeholders suggested that each country establish a data protection authority for enforcement purposes. Certain ASEAN countries currently lack such a commission. Also not yet determined is the accreditation of the certification bodies and dispute resolution and recourse mechanisms. Lab participants explained that regulators, for whom neutrality is imperative, may hesitate to provide certification lest it is perceived as an endorsement of specific CSPs or services.

A regional certification program should also accommodate local, small, and different types of CSPs, including those that handle non-sensitive data. Lab participants pointed to the announcement by the Signals Directorate of the Australian Government on March 2, 2021, that it was terminating its Cloud Services Certification Programme (which certified cloud vendors for government agency contracts). In part, this termination aimed to "open up the Australian cloud market to allow for more home-grown Australian providers to operate."[15]

SOLUTION: Hybrid and Pooled Audits

The regulatory gaps in the specialized knowledge and skills associated with cloud technology may be pronounced in some cases. A major concern among regulators is their ability to conduct a sufficiently thorough CSP audit themselves or outsource the work reliably. They must understand the operations, technologies, physical infrastructure, tasks, and procedures in place to maintain data integrity, system security, and operational continuity—a steep learning curve even for those within a firm. Lab participants were in broad agreement that audits must play an integral role in overall risk management and acknowledged that the regulatory community has grown more understanding in recent years of the challenges inherent in cloud adoption. But participants also recognize that audits can be disruptive to the CSP and potentially counterproductive if their physical access to a data center creates an additional security risk.

One suggestion to help streamline the audit process is to ensure CSPs acquire certification for common international standards such as information security, cloud security, and data privacy standards (the ISO/IEC 27000-series). This certification need only be done once and stays valid for three years.

A two-step approach, a hybrid audit, and a pooled audit could also help achieve balance for regulators and those undergoing the audits. For the *hybrid audit*, Lab participants explained, the regulator and institution separate the aspects of the CSP audit that can be conducted virtually from those that require in-person review (e.g., data center cabling and building security). Once stakeholders establish the audit components that require in-person review, a *pooled audit* can take place. This would entail a pool of participating FIs that share the costs and reduce CSP disruption by agreeing to have their on-site audits conducted together. This approach requires close coordination and flexibility among regulators, FIs, and CSPs. But it can help minimize the data center disruptions and related security risks and reduce audit costs for individual FIs.

Recommendations for Next Steps

- Industry stakeholders or trade associations should establish a regional working group to develop a risk-based data classification standard that employs existing industry data models. Additionally, the working group should design a framework for virtual and pooled audits. Stakeholders should agree on practical aspects for in-person audits and virtual audits. The working group would circulate the proposals for consultation among regional regulators.

BARRIER: Data Localization

Data localization policies require that data storage, management, and movement to IT infrastructure be limited to specific jurisdictions, often within a nation's borders. In short, if it originates there, it stays there. Most countries (and politically aligned member states, like the EU) with data localization regulations cite general principles of personal data privacy protection and the ease of regulator/law enforcement access to data centers.[16] These are the principles the Lab addressed. From a regulatory perspective, national data security is a top priority. Citizens' data stored in offshore data centers can undermine domestic regulatory authority or subject it to time-consuming disputes with another country's laws, impeding investigatory and recovery missions in times of crisis. An economic argument is made, as well, that data is a domestic commodity with national security considerations and can generate value for local industries.[17] Of eight countries in the world to impose data localization requirements, five (including India, Indonesia, and Vietnam) are located in Asia.[18] The extent of data localization requirements varies across countries, and the financial sector is usually included in these restrictions due to the sensitivity of their data.

All these reasons for localization are hard to dispute. Yet the financial sector may find that data localization policies result in unintended, unwelcome consequences:

1. Data localization can be expensive, onerous, and labor-intensive because the security standards of local CSPs and data centers may not meet corporate or third-country standards.[19] To operate locally, FIs will have to set up local infrastructure, which can require up to tens of millions of dollars in investments. The additional costs can force FIs to exit or avoid specific markets completely.[20]

2. Global restrictions on e-commerce networks and reduced capabilities to synthesize large datasets may cause FIs to refrain from using cloud computing capabilities fully.[21] Again, this may stifle investments in the local economy and hurt economic development.[22]

3. Reduced regulatory oversight may mean greater vulnerability to cyberattacks, fraud, money laundering, or terrorist financing. Inconsistent data regulations may result in limited information sharing between countries and persistent legal tension between foreign and local regulators.[23]

4. Firms may duplicate their data to work around these regulations, thus increasing the number of risk exposure points.[24]

In sum, while localization seeks to address essential goals of enhancing national cybersecurity and facilitating law enforcement, the unintended consequences may harm economic development and fail to safeguard the integrity and privacy of the country's financial data. Lab participants discussed several alternative approaches.

SOLUTION: Contractual Mechanisms for Access to Data

Contractual access (e.g., through digital trade agreements) can grant regulatory authorities access to data stored outside their jurisdictions. Contracts between countries may include clauses to facilitate cross-border data transfers and ensure that regulators have timely access for investigatory, supervisory, and crisis management purposes. In addition, countries can stipulate that they will align digital rules and standards for enhanced interoperability and data protection regimes that will not change or affect the ability of either country to enforce its existing data regulations.

One such cross-border agreement to fight terrorism and cybercrime is the UK-US CLOUD Agreement, signed in October 2019 and falling under the existing US Clarifying Lawful Overseas Use of Data Act (CLOUD Act), by which the two countries can comply with law enforcement requests for data from service providers.[25] The Australia-Singapore Digital Economy Agreement of December 2020 also addresses and updates robust bilateral data transfer rules and a comprehensive framework for digital trade facilitation without requiring the use of local-only data centers.[26] Both agreements respect the domestic laws and regulations on preserving and disclosing data.

SOLUTION: Technology-Based Controls

Technology-based controls can also help restrict unauthorized access of data. CSPs offer a range of services that allow regulators and financial institutions to control data access. For example, technical controls can enable sustained data and tenant (client) segmentation and limit access to financial data.

New confidential computing technology can also protect critical data through encryption, even while processing or using the data. This encryption adds a layer of insurance because even a CSP can't access the sensitive information that it hosts.

TABLE 1: TECHNICAL CONTROLS TO MITIGATE UNAUTHORIZED ACCESS TO DATA

Access Perimeter Policies	***Customer-Managed Encryption Services***	***CSP Administrator Access Controls***	***Automated Threat Detection Services***
Allows customers to restrict user access to data beyond defined locations and regions and prevents data removal or storage beyond authorized boundaries.[27]	Customers create, replace, and retire encryption keys according to their frequency of use and needs, which CSPs will not access.[28]	Limits CSP access by requiring approval or identification through multi-factor authentication unless access to customer content is required to resolve outage, legal, or security-related situations.[29]	Uses machine learning to monitor and flag suspicious access patterns and potential breaches in data.[30]

Source: Google Cloud (2019), Google Cloud (2020), Amazon Web Services (2020)

SOLUTION: Digital Sovereignty and Data Embassies

For the past decade, digital sovereignty, which is less restrictive than data localization, has been generally defined as the capacity of states to enforce their laws over data created by their citizens (i.e., "to assert control on infrastructures residing within their territory and data produced by their citizens"). It encompasses technology, data, and digital footprints.[31] Arguing for the rights of citizens and firms to have control over their digital destinies and for control over data as a valuable global commodity, Europe, in particular, has taken the lead in the campaign for state digital sovereignty, and even, as some contemplate, for potential supranational (EU) sovereignty.[32]

Technological advances have blurred the line between the physical and virtual. The example of Estonia shows how digital sovereignty can help countries achieve greater technological autonomy—even if data is stored offshore and distributed over the cloud. In 2017, a decade after a series of cyberattacks took down dozens of state and commercial websites in Estonia, the country became the first in the world to establish a "data embassy" (i.e., a data center in a second country). Located in Luxembourg, the data embassy has all the rights accorded a diplomatic embassy and operates under absolute Estonian control.[33] It uses Tier 4 (the highest) blockchain security and stores 10 government datasets: an "e-file (court system), treasury information system, e-land registry, taxable person's registry, business registry, population registry, State Gazette [the official online publication of state affairs], identity documents registry, land cadastral [tax surveys] registry, and the national pension insurance registry."[34] Of interest, the government explored a public-private cloud partnership in 2014 but ultimately elected instead to maintain full control over its IT infrastructure and data.[35]

Lab participants felt that this approach, while intriguing and ambitious, requires high levels of trust across jurisdictions and may be a later goal for the Southeast Asia region.

Recommendations for Next Steps

- To avoid the unwelcome and unintended consequences of data localization regulations, governments may review and amend current bilateral trade agreements to include cross-border data access for the financial sector.
- Regulators and FIs should conduct stress tests to apply specific technology-based controls and assess the extent to which these measures satisfy data, security, and privacy regulations.
- A regional stakeholder group may design a model that translates the concepts of data sovereignty and data embassies to the Southeast Asia environment, working within the contours of the region's political and regulatory landscape.

BARRIER: Cloud Concentration Risk

Cloud concentration risk refers here to the over-reliance of a financial institution on a single CSP to support all its banking services. The concentration of data management, operations, financial transactions, and IT hardware in one provider produces two kinds of challenges: firm-specific and systemic, notes Cloudera, an enterprise data CSP. The high concentration of financial clients at the firm-specific level can make the CSP a more attractive target for bad actors. Also, "vendor lock-in" can reduce competition and innovation; and because there isn't a regional framework, different exposures and rules of governance come into play. At the systemic level, the high concentration of many institutions utilizing very few CSPs presents a risk for the stability of the overall financial system.[36]

Meanwhile, Gartner finds that the top five CSPs offering IaaS in 2019 accounted for 80 percent of the public cloud market.[37] The COVID-19 pandemic has intensified the trend as FIs race to digitalize operations only to find that the CSP market has few major players. Few regulators have addressed concentration risk.

Lab participants noted the complexity and risk associated with third-party vendor supply chains and the difficulty for regulators to measure concentration risk accurately. Some Lab participants suggested breaking down the definition of concentration risk further to define infrastructure, geographical, and geopolitical risk. This clarification helps avoid conflation of quite different risks that would require clear and specific solutions. It will also help to decide who should manage the risk.

SOLUTION: Multi-Cloud and Exit Strategies

A multi-cloud strategy uses different kinds of cloud platforms and various cloud providers and is a strategy banks have popularized.[38] The multi-cloud may improve operational resilience by building on interoperability and the portability of banks' data and applications. Lab participants cited an additional advantage of the multi-cloud approach: Banks can leverage the strengths of different CSPs to address corresponding needs. By reducing the dependence on a single provider, they can avoid concentration risk and lower the likelihood of industry-wide vulnerability.

Other participants noted the need for careful implementation of a multi-cloud strategy. Setting up and managing the various cloud infrastructures for a single application may be costly and difficult to maintain and require additional recruitment and training. FIs might prefer a modified version of the multi-cloud strategy—a poly-cloud approach that distributes targeted workloads across different CSPs. This approach reduces redundancies and data duplication while retaining the benefits of multiple CSPs. Nonetheless, most participants agreed that having clear exit strategies will mitigate concerns of concentration risk. Many FIs have exit plans in place and written into contracts with CSPs. But for FIs working with a single cloud provider, an

exit may be a last resort because significant core infrastructure and applications have been invested in the technology. In this case, a gradual shift towards a multi-cloud would be necessary.

SOLUTION: Regional Industry-Specific Cloud

Another proposal is a secure regional industry-specific cloud. The cloud's default settings would incorporate regulations of individual countries, reducing ambiguity and dissonance of cloud-related rules across jurisdictions. This kind of approach offers a good balance between the CSPs' need to scale and the institutions' specific needs while providing confidence to regulators of the security of the stored financial data.

While the idea of supporting the growth of non-US and non-China-based clouds sparked interest among participants, most felt Asia is not ready for a plan like the EU's seven-year, €10 billion public-private investment to develop domestic CSPs and a federated cloud.[39] Moreover, there was some doubt that government-led initiatives could match the flexibility and initiative that today's CSP "hyperscalers"—the CSPs developed by Alibaba, Amazon, Google, and Microsoft—lived and breathed in their early development years. Instead, regional financial centers, such as Singapore, could serve as hubs for a regional cloud.

Recommendations for Next Steps

- Regulators should identify various types of risk (e.g., infrastructure, geographic, and geopolitical), making them easier to benchmark and monitor.
- Institutions could consider a poly-cloud strategy and engage the services of the appropriate CSPs for specific parts of an application or workload to become more resilient to concentration risks. A multi-cloud approach would step in where one or two CSPs dominate particular workloads or processes (e.g., in email and office-related software).
- CSPs keen to explore a regional industry-specific public cloud should work with national banking associations or a regional financial hub to identify institutions with a similar interest.

CONCLUSION

The benefits of cloud-based technology and services for the financial industry were clear before the COVID-19 pandemic, as evidenced in the decade-long shift into e-commerce and other digital operational functions and transactions. But the past year and a half have been a tipping point. Quick shifts in business processes and accelerating the deployment of new products and services through cloud technology improved the financial sector's resilience to some extent. With more global FIs moving to the cloud, we encourage Southeast Asia industry leaders to learn the cloud basics, be mindful that technology training never stops, and recognize that binding contracts and agreements build trust across borders.

Our Financial Innovations Lab participants from diverse fields and regions have helped chart a path forward to better enable regulatory compliance. Steps include developing a regionally accepted data classification scheme, designing a CSP certification system, and using hybrid and pooled audits. We explored contractual and technology-based pathways to reduce the need for data localization laws. Finally, we described how a multi-cloud approach, clear exit strategies, and a regional industry-specific public cloud could help address concentration risk. The Milken Institute will continue to engage with experts and stakeholders on this topic and provide a platform for testing solutions.

ENDNOTES

1. "Public Cloud Adoption in Financial Services" (Celent, July 8, 2020), www.ibm.com/downloads/cas/A2YBMXWZ.
2. Alan McIntyre et al., "The Cloud Imperative for the Banking Industry" (Accenture, September 29, 2020), www.accenture.com/us-en/insights/banking/cloud-imperative-banking.
3. Roland Rajah, "Southeast Asia's Post-Pandemic Recovery Outlook" (Brookings Institution, March 15, 2021), www.brookings.edu/blog/order-from-chaos/2021/03/15/southeast-asias-post-pandemic-recovery-outlook/.
4. Liam Eagle, "Multi-Cloud Fundamental to Financial Services Transformation" (451 Research, January 2019), www.information-age.com/downloads/multi-cloud-fundamental-to-financial-services-transformation/; Craig Balding et al., "Cloud Usage in the Financial Services Sector Banking on the Cloud: Real-World Use, Challenges and Opportunities across the Banking and Finance Sector" (Cloud Security Alliance, February 21, 2020), https://cloudsecurityalliance.org/artifacts/cloud-usage-in-the-financial-services-sector/.
5. "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021," Gartner, November 17, 2020, www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021.
6. Alan McIntyre et al., "The Cloud Imperative for the Banking Industry."
7. "38% Growth in Asia-Pacific Public Cloud Services Spending," *SMEhorizon*, March 18, 2021, www.smehorizon.com/38-growth-in-asia-pacific-public-cloud-services-spending/.
8. Aaron Tan, "China's Cloud Infrastructure Spending Hits Record Growth," *Computer Weekly*, March 25, 2021, www.computerweekly.com/news/252498396/Chinas-cloud-infrastructure-spending-hits-record-growth.
9. "Proposed ASIFMA Principles for Public Cloud Regulation" (Asia Securities Industry and Financial Markets Association, March 2021), www.asifma.org/wp-content/uploads/2021/03/final-proposed-asifma-principles-for-public-cloud-regulation.pdf.
10. "Better on the Cloud Financial Services in Asia Pacific" (Asia Cloud Computing, 2021), www.slideshare.net/accacloud/acca-better-on-the-cloud-financial-services-in-asia-pacific-2021.
11. "Amendments to Regulations on Outsourcing and IT Risk Management," Banko Sentral NG Pilipinas, accessed July 15, 2021, www.bsp.gov.ph/Regulations/Issuances%20of%20Policy%20Exposure%20Drafts/Draft_Circular_Amendments_to_the_Outsourcing_Policy_of%20_the_MORB_31May.pdf.
12. Ryan Brooks, "Data Classification for Compliance: Looking at the Nuances," *netwrix Blog*, June 4, 2021, https://blog.netwrix.com/2020/03/17/data-classification-for-compliance/.

13. "Data Classification: Secure Cloud Adoption." (Amazon Web Services, March 2020), https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf.
14. "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories" (National Institute of Standards and Technology, US Department of Commerce, August 2008), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.
15. Aaron Tan, "Australian Government Pulls Plug on Cloud Certification Programme," *Computer Weekly*, March 5, 2020, www.computerweekly.com/news/252479572/Australian-government-pulls-plug-on-cloud-certification-programme.
16. Pablo Urbiola et al., "Data Flows across Borders Overcoming Data Localization Restrictions" (Institute of International Finance, March 2019), www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf; Farid Gueham, "Digital Sovereignty: Steps towards a New System of Internet Governance" (Fondation pour L'Innovation Politique, February 2017), www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/.
17. Pablo Urbiola et al., "Data Flows across Borders Overcoming Data Localization Restrictions."
18. Jun Ishihara, "Asian Countries Build Data Fortresses to Protect New National Assets," *Nikkei Asia*, November 26, 2020, https://asia.nikkei.com/Spotlight/Century-of-Data/Asian-countries-build-data-fortresses-to-protect-new-national-assets.
19. "How the Trend towards Data Localisation Is Impacting the Financial Services Sector" (International Regulatory Strategy Group and DAC Beachcroft LLP, December 2020), www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf.
20. James M. Kaplan et al., "Addressing the Impact of Data Location Regulation in Financial Services" (Global Commission on Internet Governance, Paper Series No. 14, May 2015), www.cigionline.org/sites/default/files/no14_web_0.pdf.
21. "Southeast Asia's Data Localisation," *The ASEAN Post*, December 2, 2019, https://theaseanpost.com/article/southeast-asias-data-localisation.
22. "How the Trend towards Data Localisation Is Impacting the Financial Services Sector" (International Regulatory Strategy Group and DAC Beachcroft LLP, December 2020), www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf.
23. Ibid.
24. Ibid.
25. Eugenia Lostri, "The CLOUD Act," Center for Strategic and International Studies, October 2, 2020, www.csis.org/blogs/technology-policy-blog/cloud-act.
26. "Australia–Singapore Digital Economy Agreement," Australian Government Department of Foreign Affairs and Trade, December 8, 2020, www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement.

27. "Data Residency, Operational Transparency, and Privacy for European Customers on Google Cloud" (Google Cloud, February 2020), https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf.
28. "Trusting Your Data with Google Cloud Platform" (Google Cloud, September 2019), https://cloud.google.com/files/gcp-trust-whitepaper.pdf.
29. Ibid; "Data Residency AWS Policy Perspectives" (AWS, August 2020), https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf.
30. Ibid.
31. Stéphane Couture, "The Diverse Meanings of Digital Sovereignty," MIT Global Media Technologies & Cultures Lab, August 5, 2020, https://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/.
32. Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Springer*, Editor Letter, August 12, 2020, https://link.springer.com/article/10.1007/s13347-020-00423-6.
33. "Data Embassy," e-Estonia, accessed August 9, 2021, https://e-estonia.com/solutions/e-governance/data-embassy/.
34. "Data Embassy: The Digital Continuity of a State," e-Estonia, December 2019, https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/.
35. "Estonia to Open the World's First Data Embassy in Luxembourg," e-Estonia, June 2017, https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.
36. Richard L. Harmon, "Cloud Concentration Risk II: What Has Changed in the Past Two Years?" (Cloudera, July 6, 2020), www.cloudera.com/content/dam/www/marketing/resources/whitepapers/cloud-concentration-risk-ii-whitepaper.pdf.landing.html.
37. "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 37.3% in 2019," Gartner, August 10, 2020, www.gartner.com/en/newsroom/press-releases/2020-08-10-gartner-says-worldwide-iaas-public-cloud-services-market-grew-37-point-3-percent-in-2019.
38. "What Is Multi-Cloud? Multi-Cloud Definition and Related FAQs," Avi Networks, accessed June 23, 2021, https://avinetworks.com/glossary/multi-cloud/.
39. Melissa Heikkilä et al., "EU Shoots for €10B 'Industrial Cloud' to Rival US," *Politico*, October 16, 2020, https://www.politico.eu/article/eu-pledges-e10-billion-to-power-up-industrial-cloud-sector/.

FINANCIAL INNOVATIONS LAB PARTICIPANTS

Brigitta Ratih Aryanti, Head of Government Affairs and Public Policy, Google Cloud Indonesia

Reuben Athaide, Head, Cloud Customer Engagement, Standard Chartered Bank

Mandar Bale, Security and Compliance Specialist, Google Cloud

Lowell Campbell, Global Digital Finance Specialist, International Finance Corporation

Marvin Castell, Senior Officer, Finance Integration, ASEAN Secretariat

Belinda Chng, Director, Policy and Programs, Milken Institute

Citra Christina, Junior Analyst, Otoritas Jasa Keuangan (OJK, Indonesia)

Neal Cross, Fintech Advisory Board Member, Razer

Jason Davis, Senior Associate, Innovative Finance, Milken Institute

Théo Cohan, Associate Director, Innovative Finance, Milken Institute

Kate Ross Goldman, FinTech Associate, Center for Financial Markets, Milken Institute

Andreas Kalkum, Director, Head of APAC Digital Private Bank, Online and Mobile Banking, Credit Suisse

Yuji Kawada, Deputy Director on Innovation Financial Technologies, Financial Services Agency Japan

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

Cheryl Low, Intern, Policy and Programs, Milken Institute

Caitlin MacLean, Senior Director, Innovative Finance, Milken Institute

Reginald Mendoza, Assistant Vice-President, Head of Emerging Technologies and Innovation Division, Philippine National Bank

Michael Morallos, Senior Vice President, Head of Technology Group, Philippine National Bank

Irawan Muhamad, Banking Research and Regulation Department, Otoritas Jasa Keuangan (OJK, Indonesia)

Barbara Navarro, Head of Government Affairs and Public Policy, Google Cloud APAC

Aninda Nusratina, Junior Analyst, Otoritas Jasa Keuangan (OJK, Indonesia)

Bintang Prabowo, Analyst, FinTech Innovation Group, OJK

Muhammad Radhi, Junior Analyst, Otoritas Jasa Keuangan (OJK, Indonesia)

Yuta Takanashi, Director for International Digital Strategy and International Policy, Financial Services Agency Japan

Ella Tan, Associate, Policy and Programs, Milken Institute

Tony Tony, Deputy Director, Department of Banking Research and Regulation, Otoritas Jasa Keuangan (OJK, Indonesia)

Anupam Verma, Chief Executive Singapore and SEA Head, ICICI Bank

Lito Villanueva, Executive Vice President and Chief Innovation and Inclusion Officer, Rizal Commercial Banking Corporation

Augustine Wong, Chief Information Officer, Vietnam Prosperity Bank

Budi Yuwono, Senior Officer ICT Sector, Infrastructure Division, ASEAN Secretariat

ADDITIONAL PROJECT CONTRIBUTORS

Jo Ann Barefoot, Chief Executive Officer, Barefoot Innovation Group

Crispin Bui, General Director, Vietnam, WorldQuant

Brad Carr, Senior Director, Digital Finance Regulation & Policy, Institute of International Finance

Yam Ki Chan, Head of Financial Services Policy, Google Cloud

Brandon Chye, Economist, Official Monetary and Financial Institutions Forum

Chuchi Fonacier, Deputy Governor of the Financial Supervision Sector, Bangko Sentral ng Pilipinas

Romain Groleau, Managing Director, AAPAC Cloud, Accenture

Tanya Hotchkiss, Executive Vice President, Cantilan Bank

Stuart Houston, Director, Financial Services, Google Cloud

Melissa Koide, Founder & Chief Executive Officer, FinRegLab

Laura Deal Lacey, Executive Director, Milken Institute

Daniel Long, Vice President, Goldman Sachs

Shailesh Naik, Founder & Chief Executive Officer, MatchMove

Eric Rabin, Managing Director & Chief Operating Officer, Asia-Pacific, Societe Generale

Anand Sachdev, Chief Executive, Westpac Singapore & Chief Operating Officer, Westpac

Rick Sherlund, Vice Chairman of Technology Investment Banking, Bank of America

Vikram Subrahmanym, Regulatory and Cross-Enterprise Transformation Lead & Strategic Projects Lead, Asia Pacific, Citi

Thurain Tun, Financial Services Industry Lead, Google Cloud

Suprita Vohra, Director, Risk Solutions Group, Barclays

ABOUT THE AUTHORS

Jason Davis is a senior associate of innovative finance at the Milken Institute. He contributes to the research, development, execution, and follow-up of our Financial Innovations Labs, which address market failures and funding gaps within social or environmental issues. During his time at the Institute, Davis has explored various topics, including financing large-scale coastal resiliency infrastructure projects in New York City. He has also studied how Los Angeles can facilitate a "green recovery" during the COVID-19-induced economic downturn and how to improve long-term care access and financing in the United States. Before joining the Milken Institute, Davis held several positions in the media industry in New York and Los Angeles. Davis graduated with a BFA from Syracuse University and recently earned his MBA from Loyola Marymount University.

Ella Tan is an associate on the Milken Institute Asia Center's Policy & Programs team. Her current research focuses on vaccination access and delivery, the opportunities and challenges for technology to transform mental health care in Asia, and the role of cloud technology to enhance resilience and advance the Environmental, Social, and Corporate Governance (ESG) goals of the financial sector. Tan is a graduate of the National University of Singapore and has an MSc (economics) from the Singapore Management University.


MILKEN
INSTITUTE