asifma

Growing Asia's Markets

Proposed ASIFMA Principles for Public Cloud Regulation

March 2021

Disclaimer

The information and opinion commentary in this ASIFMA – *Proposed ASIFMA Principles for Public Cloud Regulation* was prepared by the Asia Securities Industry and Financial Markets Association (**ASIFMA**) to reflect the views of our members. ASIFMA believes that the information in the Paper, which has been obtained from multiple sources believed to be reliable, is reliable as of the date of publication. As estimates by individual sources may differ from one another, estimates for similar types of data could vary within the Paper. In no event, however, does ASIFMA make any representation as to the accuracy or completeness of such information. ASIFMA has no obligation to update, modify or amend the information in this Paper or to otherwise notify readers if any information in the Paper becomes outdated or inaccurate. ASIFMA will make every effort to include updated information as it becomes available and in subsequent papers.

ASIFMA is an independent, regional trade association with over 140 member firms comprising a diverse range of leading financial institutions from both the buy and sell side including banks, asset managers, accounting and law firms, and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the U.S. and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

Contents

I. Introduction to the public cloud

Cloud computing offers an adaptable and versatile way to consume a range of information technology ("IT") services, such as business applications, data storage or processing power. Cloud is offered 'as a service', where IT resources are provided on-demand and the location of the physical hardware and application are largely extraneous to the users. Cloud computing is rapidly becoming the norm for IT processing and data storage solutions and is offered both by major and niche vendors.

In this paper, we are focusing on public cloud. In a public model, cloud infrastructure is provisioned for open use by multiple organisations. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the Cloud Service Provider ("CSP")[1].

Whilst all cloud models and services are important for financial institutions ("FIs"), the use of public cloud is of greater interest and scrutiny within the industry today largely because of the increasing adoption of public cloud within the industry (both by FIs and their third-party providers), and the differentiators associated with public cloud versus other models (private cloud or traditional on-premises IT).

Shared responsibility model

Public cloud has different implications for the responsibilities of FIs and CSPs, for areas such as management of data centres and infrastructure (e.g., servers), security (e.g., data access), and risk and compliance (e.g., the applicability of regulatory requirements). Known as 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 centre facilities, whilst the FI is responsible for aspects such as customer data, security, application management and user access. This model can also extend to sharing responsibilities for IT controls and risk management requirements (for example, both parties owning and managing access controls for areas which they are responsible for). Nevertheless, this shared responsibility model does not mean that FIs discharge their ultimate accountability on CSPs, as the ultimate liability for any FI activity will always be held by the FI.

[1]AFME (2019): The Adoption of Public Cloud Computing in Capital Markets https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20Cloud%20Paper%20November%202019%20Final.pdf

Benefits of public cloud

The use of public cloud brings significant benefits[2] to the financial services industry in the areas of risk mitigation, innovation, cost savings and productivity gains:

Risk Mitigation

- Effective risk mitigation, such as increased operational resilience, to ensure continuity of service by distributing the risk of disruption across a greater range of infrastructure, both on-premises and off-premises;
- Compared to on-premises environments, the locational diversity of CSPs' infrastructure greatly reduces geographic concentration/systemic risk;
- Benefit from the cybersecurity capabilities and tools of the CSPs who invest billions in advanced cybersecurity capabilities and tools, thus offering better protection;
- Cloud offers FIs the capability to architect and build workloads that are able to withstand outages and security threats.

Innovation

- Greater business agility and innovation, providing computing capacity for experimentation and development (Platform as a Service ("PaaS"), Software as a Service ("SaaS")), reducing project lead times, and increasing scalability. Flexible usage allows FIs to run IT workloads or applications as required, such as developing reports or data analytics, without needing to retain a large IT footprint (Infrastructure as a Service ("IaaS"), PaaS, SaaS);
- Access to advanced technologies and capabilities, such as data analytics, machine learning and artificial intelligence ("AI"), which FIs cannot get in any other way, or at the same cost, quality and speed. These advanced technologies enable FIs to deliver better products and services to their customers, improve their ability to fight financial crime and manage risk;
- Enhanced client experience and service offerings, quickly developing, testing, and rolling out new products or features to FI's functions and clients;
- Cloud can help FIs achieve their sustainability goals. With fewer data centres and use of more shared resources through the use of cloud, FIs can improve their sustainability credentials.

Cost savings

- Reduced spend on procuring physical hardware and facilities, such as on-premises data centres and the associated operations and maintenance required, by moving to on-demand usage of services on a pay-as-you-go basis (e.g., IaaS, PaaS and SaaS) frees up resources for upgrades to infrastructure and digital capabilities, which ultimately results in better services for clients;
- Improved overall cost management, as cloud adoption is generally a business-wide strategy rather than at the level of individual business units (although adoption may start within specific

[2]AFME (2019): The Adoption of Public Cloud Computing in Capital Markets
https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20Cloud%20Paper%20November%202019%20Final.pdf

functions). Consumption can be monitored at a granular level, providing greater transparency and control.

Productivity gains[3]

- Increased operational efficiency, allowing for increased speed and agility in existing IT and operations processes, through greater automation and self-service tools;
- Higher team productivity by providing access to proven tools that IT teams can use to develop systems. In addition to improved productivity in non-IT functions, using cloud-enabled analytics and other advances such as AI and machine learning, organisations are able to improve decision making, leading to greater cost efficiencies;
- The public cloud allows users to take new products and services to market quickly.

How public cloud can enhance operational resilience

The role cloud can play in enhancing operational resilience became even more prevalent in 2020 in light of the Covid-19 pandemic. As the pandemic evolves, the FI services industry is increasingly focusing on digitisation in which cloud plays a key enabling role. Indeed, the ongoing Covid-19 situation has proven that cloud can help organisations improve their operational resilience in different ways. It has allowed the whole industry to be more resilient, to effectively manage operational risks, and ultimately to be 'part of the solution' to recover from the pandemic:

- CSPs' core business is to provide a **highly resilient infrastructure** to protect against hardware failures, natural disasters, power outages and threats. To achieve this, CSPs make considerable investments in security and to develop best in class protections.
- CSPs rely on geographically distributed data centres located far apart, and isolated from each other across zones and regions, thereby **minimising the risk of contagion and single point of failure.**
- The redundant nature of cloud, which basically means the CSP having more than one 'copy' of data, systems and equipment across regions, **ensures the availability and continuity of systems and services** even in the event of unexpected failures. This is further reinforced by the possibility to transfer data, including critical functions, between server locations.
- Cloud elasticity allows for a very flexible, customised and real- time use by FIs who can react instantly and efficiently to market conditions. In response to peak demands, they can **easily scale up with minimised service disruptions** and without the need for on-site physical presence. This has been absolutely crucial in the pandemic situation, where both employees, through increased and secure remote working capabilities, and customers, through secure and reliable digital access to banking, were positively impacted.
- **Cybersecurity**: the controls and security protocols of the CSPs complement and further enhance those of FIs.

[3] BCG (2019): Ascent to the Cloud: ow Six Key APAC Economies Can Lift-off Ascent to the Cloud: How Six Key APAC Economies Can Lift-off (bcg.com)

Regulatory support for public cloud

Regulators in the region already recognise the benefits of cloud, e.g., the Monetary Authority of Singapore ("MAS") in Section 6.2 of their Guidelines on Outsourcing: "*[Cloud services] can potentially offer a number of advantages, which include economies of scale, cost-savings, access to quality system administration as well as operations that adhere to uniform security standards and best practices. [Cloud services] may also be used to provide the flexibility and agility for institutions to scale up or pare down on computing resources quickly as usage requirements change, without major hardware and software outlay as well as lead-time. In addition, the distributed nature of [cloud services] may enhance system resilience during location-specific disasters or disruptions.*"[4]

The European Securities and Markets Authority ("ESMA") in their 'Guidelines on outsourcing to cloud service providers[5]' in paragraph 2: *"Acknowledges that cloud outsourcing can bring benefits, including enhanced flexibility, operational efficiency, and cost effectiveness, with potential positive outcomes for firms and investors."* ESMA had adopted many principles of the European Banking Authority's ("EBA") recommendations under its 'Recommendations on outsourcing to cloud service providers[6]' report that detailed in paragraph 4 that *"Cloud outsourcing services are much more standardised, which allows the services to be provided to a larger number of different customers in a much more automated manner and on a larger scale."* And that "*Cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness."*

The Basel Committee for Banking Supervision describes cloud as an "enabling technology" that provides the underlying infrastructure for many FinTech activities and other technology solutions[7] utilised by the financial services industry.

The International Organisation of Securities Commissions ("IOSCO") in its May 2020 Consultation on the Principles of Outsourcing[8] highlights several advantages of cloud-based infrastructures, including improved accessibility, cost efficiency, demand scalability, always-on availability, and improved security.

[4] MAS (2016): Guidelines on Outsourcing https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf

[5] ESMA (2020): Guidelines on outsourcing to cloud service providers esma50-157-2403_cloud_guidelines.pdf (europa.eu)

[6] EBA (2017): Final Report – Recommendations on outsourcing to cloud service providers EBA BS 2017 XX (Final draft Recommendations on Cloud Outsourcing).docx (europa.eu)

[7] BCBS (2018): Sound Practices: implications of fintech developments for banks and bank supervisors Sound Practices: implications of fintech developments for banks and bank supervisors (bis.org)

[8] IOSCO (2020): Principles on Outsourcing – Consultation Report https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf

Regulators have also recognised the role that cloud can play in enhancing the sector's operational resilience, e.g. the UK Prudential Regulation Authority in their ongoing 2019 consultation paper[9] on outsourcing and third party risk management in paragraph 1.9: "*These changes in firms' reliance on outsourcing and third parties bring potential benefits and opportunities, including, in the case of Cloud, potentially enhanced resilience compared to firms' on-premise data centres (provided that firms oversee the provision of Cloud services effectively and take appropriate steps to protect their applications and data)".*

II. Regulatory fragmentation creating challenges to cloud adoption

Whilst the above benefits of public cloud are recognised, adoption and implementation of public cloud by FIs can be complex due to sometimes conflicting regulatory requirements. Regulators diverge on approaches to regulation of public cloud services and CSPs driven by views of innovation risk, national sovereignty, competition and systemic risk, all of which contributes to FIs having to manage their CSPs in a fragmented way, to address such jurisdictional differences.

For FIs that have decided that cloud will be part of their (global) strategy, there continue to be considerable hurdles caused by differing regulatory frameworks across jurisdictions, both specific to financial services, as well as regulation and legislation targeting data privacy and security[10]. The challenges stem from inconsistent requirements (e.g. around audit and cybersecurity), and varying regulatory frameworks, ranging from treating cloud as being automatically a form of outsourcing (e.g. MAS consultation on Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services[11]), to treating cloud as critical third-party service providers (e.g. the draft EU Digital Operational Resilience Act[12], the Korean Financial Services Commission ("FSC") Proposed amendments to the Electronic Financial Transactions Act[13]) and considering oversight of CSPs.

[9] BOE (2019): Outsourcing and third party risk management - https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf?la=en&hash=4766BFA4EA8C278BFBE77CADB37C8F34308C97D5

[10] ASIFMA (2020): Addressing Market Fragmentation Through the Policymaking Lifecycle https://www.asifma.org/wp-content/uploads/2020/08/asifma-fragmentation-paper-f20200804.pdf

[11] MAS (2020): Consultation Paper on Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services Consultation Paper on Notices to Banks and Merchant Banks on Management of Outsourced Relevant Services (mas.gov.sg)

[12] European Commission (2020): Draft regulation on Digital Operational Resilience for the financial sector https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

[13] Korea FSC (2020): 의안정보시스템 (assembly.go.kr)

Examples of regulatory challenges include:

- Rule-based (versus risk-based) prescriptive framework on cloud adoption in many jurisdictions which impedes a uniform cloud-based architecture deployment, needed to support a global network;
- Differing standards and regulatory requirements across jurisdictions on materiality/criticality thresholds, data protection, encryption requirements, approval requirements, third-party audits, risk governance, certifications, requirements on access by regulator to data stored on public cloud etc. Public cloud strategies are global so these regional or local differences and inconsistencies are problematic as they will lead to a fragmented architecture for FIs resulting in increased complexities and risk;
- Data localisation requirements (or regulations amounting to 'de facto' data localisation requirements) which leads to restrictions on cloud locations and ownership of CSPs;
- Lack of level-playing field due to inconsistent requirements for FIs, digital banks and 'BigTechs';
- Regulators' concerns regarding the resilience of CSPs, market concentration and the potential impact of CSPs on financial stability;
- Hindrance to cloud adoption due to at times challenging outsourcing regulations including for example complicated and lengthy regulatory notification/approval requirements.

III. ASIFMA's proposed principles for public cloud regulation

Whilst authorities and regulators generally acknowledge the advantages public cloud can bring, they are at the same time concerned about concentration risk, data access, cybersecurity and resilience. Regulators regionally have been taking different approaches to addressing these concerns with some regulators taking a supportive stance and others implementing certain requirements pertaining to public cloud that can present blockers to adoption.

Recognising that there is a growing need regionally for an aligned approach for the regulation of public cloud to better serve consumers and markets without compromising the core regulatory objectives of protecting consumers and systemic stability, we outline in this paper nine suggested high-level principles to public cloud regulation.

Principle 1: Recognising the benefits of public cloud
Principle 2: Supporting ongoing dialogue
Principle 3: Supporting technology-neutral and activity-based regulation
Principle 4: Supporting harmonisation of public cloud requirements
Principle 5: Supporting a principles-based and outcome-focused approach to cloud regulation
Principle 6: Risk assessment and due diligence of public cloud arrangements and CSPs
Principle 7: Supporting free movement of data
Principle 8: Approval and notification requirements
Principle 9: Concentration risk

ASIFMA and its members look forward to discussing these principles with regulators and authorities in Asia and globally. We hope these principles can inform the conversation, facilitate the dialogue between FIs and policy makers, drive regulatory harmonisation and support adoption of public cloud in the financial services industry whilst also addressing regulators' concerns.

Principle 1: Recognising the benefits of public cloud

Regulators should recognise and embrace the benefits (see section I) that public cloud can bring and the financial services industry should be empowered to make use of cloud services in a way that is compatible with local laws and regulations. We expect that in the foreseeable future, cloud technology will become the norm. Any regulatory development will need to keep pace with the trend to ensure that the financial services industry can take advantage of technology efficiently to maintain a competitive edge and leverage the risk and resiliency benefits that cloud provides, as compared to the maintenance of legacy infrastructure.

Principle 2: Supporting ongoing dialogue

Regulators, the financial services industry and CSPs should have an ongoing open dialogue. We encourage regulators to facilitate and/or participate in multi-stakeholder public-private technology forums and 'compliant by design' solutions, to aid in early identification and resolution of key regulatory issues and concerns. We also encourage regulators to play a proactive role in clarifying misconceptions, certainly in jurisdictions where there is no clarity on whether the use of cloud is allowed (e.g. for sensitive or core workloads) or subject to which conditions.

Principle 3: Supporting technology-neutral and activity-based regulation

Regulators should support technology-neutral and activity-based regulation to ensure a level playing field and to support innovation and technology adoption. A competitive level playing field is needed to ensure all firms involved in the financial services industry adhere to the principle of 'same activity, same risk, same regulation'. A level playing field for all financial services industry participants is essential to manage risk, whilst supporting competition and innovation. This means that existing regulation should be deployed and applicable to entities who may currently be outside the financial services regulatory framework but are conducting the same or similar activities as regulated FIs.

Principle 4: Supporting harmonisation of public cloud requirements

Regulators should support greater regional and global harmonisation in public cloud requirements and supervisory practices by promoting a consistent and globally aligned framework for authorisation, implementation management and reporting, in order to remove barriers to adoption. Such regulatory alignment and coordination can be managed through global supervisory colleges, supervisory information sharing and collaboration with the aim to prevent disparate regulatory requirements which are resource-intensive to comply with and can distract from the fundamental management of risks. In the absence of harmonisation of regulatory principles and frameworks across geographies, we suggest regulators explore

reliance on equivalence, deference or substituted compliance decisions, and more reliance placed on home supervisor supervision of multi-national institutions.

Regulatory coordination and dialogue at the global level is essential to design common principles and approaches to cloud regulation and rules that could then be implemented nationally to avoid fragmentation as much as possible. FSB and IOSCO are well placed to play this coordinating role and convene meaningful discussions for a for multi-stakeholder exchange to include supervisors, policymakers, FIs and CSPs. Common approaches to risk assessment and control frameworks recognised by regulators and/or international sector-specific certification schemes could also be beneficial to create assurances to the industry.

Whilst the debate around direct financial regulatory oversight of CSPs is evolving, regulators need to consider that any direct oversight initiative should not become a barrier for competition in the market, eliminating the providers who cannot afford the costs of regulatory oversight compliance and leaving only the big players in the market.

Any local/regional approaches to public cloud regulation could pose significant challenges to FIs operating across borders. For example, limitations in one region may make the deployment of a global process to a certain service provider impossible. If regions diverge in their limitations regarding different providers, then there may be no providers with which FIs could work on a global level. While outright bans remain unlikely, different approval processes or IT security requirements placed on the providers may result in regulatory risk that defeats the business case for such activities. Such an outcome would form a regulatory barrier to innovation and the modernisation of FIs' IT estates resulting in continued complexity, including greater reliance on end-of-life systems, and ultimately greater risk.

Principle 5: Supporting a principles-based and outcome-focused approach to cloud regulation

Any regulation pertaining to FI's usage of public cloud should be principles-based and outcome-focused, taking into account the cross-border nature of cloud and to enable the financial services industry to implement it practically. Such principles-based approach will avoid regulation becoming stale as technology changes and will avoid the need to finetune/add on adjuncts which can lead to overly complex regimes. It will also provide the flexibility needed for FIs to implement the appropriate controls for the activities they are conducting in a risk-based and proportionate manner, which is important for FIs. By basing their controls and compliance on an analysis of the risk posed by any activity or process, FIs can design mitigation strategies tailored to the specific risk and which allow the flexibility needed to account for the possible decrease or increase in risk posed by the activity.

- Regulators should refrain from micromanaging cloud adoption and refrain from introducing a new risk category for cloud, and instead focus on systemic issues and resilience and seeking assurance in financial service's pre-existing governance, information security and outsourcing requirements.
- Regulators should ensure adequate transparency in their principle-based requirements and their regulatory expectations for FIs' cloud adoption. Regulators should also ensure consistent and transparent application of the principles (e.g., refrain from imposing additional or obscure

requirements during the course of regulatory examinations where these requirements are not part of the written regulation).

- We recommend an accountability-driven approach, where regulators specify the principles around managing/mitigating risks relating to cloud usage, and leave it to FIs to implement the principles within existing frameworks, such as third-party risk management or outsourcing requirements, IT risk management requirements, disaster recovery/business continuity management requirements and/or privacy laws, in order to create the security measures/framework to be adopted for public cloud.
- Regulators should allow FIs to assess the specific cloud services they intend to use to determine whether they are outsourcing, by leveraging existing assessment frameworks. Each cloud arrangement should be subject to an assessment for identifying the particular risk attributes such as service, scope and infrastructure, involved. If all cloud models (e.g., SaaS versus IaaS) were to be treated in the same way and subject to heightened regulations, such regulations may stifle the ability to realise the benefits of cloud technology, while not being commensurate with the relevant risks. A blanket designation that all usage of public cloud is outsourcing, for example, is not a sensible approach as it does not take into account real risk, which should be determined by the use case and the data classification.

Principle 6: Risk assessment and due diligence of public cloud arrangements and CSPs

- Regulators' due diligence requirements for FIs should focus on the control objectives/outcome and should not prescribe specific requirements or controls.
- FIs should perform appropriate due diligence on CSPs and should leverage existing supplier guidelines/regulations and technology risk management guidelines for guidance on the risk assessment and due diligence requirements of public CSPs.
- Regulators should allow FIs to use certifications based on international standards and independent or external (pooled) audits/assessments which can be conducted regularly and shared with regulators and clients to facilitate the due diligence process of CSPs. Further, use of joint industry audits or other collaborative reviews of CSPs could reduce the burden on FIs and CSPs of duplicative information requests where a CSP serves common FI clients. Such audits have taken place successfully in recent years in Germany.14
- Subcontracting: We suggest that due diligence conducted in respect of a sub-contractor should be of a standard that is proportionate to the risk involved and should not be at the same level of detail and scrutiny as compared with due diligence conducted of a CSP which is directly contracted by a regulated entity. In many instances, regulated FIs would not be granted the same level of direct access to the sub-contractors for the purpose of undertaking due diligence. Furthermore, regulated FIs generally have the contractual benefit of its service providers being liable for the services provided by its sub-contractors.

[14] BaFin (2020) https://www.bafin.de/SharedDocs/Downloads/EN/BaFinPerspektiven/2020/bp_20-1_cybersicherheit_en.pdf?__blob=publicationFile&v=5 referring to the establishment by Deutsche Börse, of the Collaborative Cloud Audit Group (CCAG) in 2017. This industry-wide initiative, involving several major European financial institutions and insurance companies, was reported in 2020 to have conducted audits of global CSPs such as Microsoft on behalf of its members.

Principle 7: Supporting free movement of data

- Regulators should support cross border data flow with appropriate controls if sensitive data is being transferred and continue to identify and remove rules and requirements which impede the ability to adopt global cloud strategies.
- Cross-border collaboration between regulators is necessary to realise regulators' legitimate right to access data for prudential and market supervision and to limit the risk of disparate and potentially conflicting data access and sharing requirements imposed by different jurisdictions.
- Regulators should focus on ensuring the FIs' relevant data remains accessible from their jurisdiction, and not on the data being stored in a specific jurisdiction. (e.g., FIs should not be required to maintain local duplicate copies of data that they store on the cloud).
- FIs should have in place adequate policies and controls to ensure that data relating to regulated activity that they are responsible for supervising remains accessible, regardless of where such data is stored. FIs should ensure proper data protection and consider all legal and regulatory considerations for the jurisdiction(s) where data is held. We refer to the ASIFMA 2019 ASIFMA Technology-Neutral Principles for Virtual Data Storage. [15]

It should be noted that imposing overly restrictive regulatory requirements for cloud use by FIs can result in "de-facto" data localisation as no cross-border operating model can satisfy such onerous and often conflicting regulatory requirements. Global FIs typically consolidate their systems in a single global hub, which offers services to the rest of the firm. In contrast, data/technology localisation policies require discrete technological builds in specific jurisdictions and further segregate local systems from global hubs. In effect, this exposes FIs to greater cybersecurity risks by creating a more decentralised environment that needs to be safeguarded, which further inhibits central oversight and information sharing across borders.

Some noteworthy supportive and enabling examples and approaches to cross-border data flow include:

- UK-Japan Comprehensive Economic Partnership Agreement[16]: According to the UK's Department of International Trade, this recently agreed trade deal will "*enable free flow of data whilst maintaining high standards of protection for personal data*" and introduce "*a ban on data localisation, which will prevent British businesses from having the extra cost of setting up servers in Japan.*"
- UK-Australia Free Trade Agreement[17]: Although this is currently being negotiated, in a position paper the UK said it "*will seek to guarantee the free flow of data and eliminate unjustified data localisation requirements*" and noted that "*[e]liminating unjustified data localisation requirements further reduces costs to businesses trading overseas, which can be prohibitive for SMEs.*"

[15] ASIFMA (2019): Technology-Neutral Principles for Virtual Data Storage 2019-06-virtual-data-storage-principles.pdf (asifma.org)

[16] UK Gov (2020) Press Release: UK and Japan agree historic free trade agreement https://www.gov.uk/government/news/uk-and-japan-agree-historic-free-trade-agreement

[17] UK Gov (2020) Policy Paper: UK-Australia free trade agreement: the UK's strategic approach https://www.gov.uk/government/publications/uks-approach-to-negotiating-a-free-trade-agreement-with-australia/uk-australia-free-trade-agreement-the-uks-strategic-approach

- US-Japan Digital Trade Agreement[18]: In the DTA the US and Japan agreed to refrain from prohibiting or restricting cross-border transfers of information "*solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of a covered person.*" According to the US Trade Representative, the agreement ensures "*that data can be transferred across borders, by all suppliers, including financial service suppliers.*"
- US-Mexico-Canada Agreement[19]: According to the US Trade Representative, this comprehensive agreement will "*[e]nsure that data can be transferred cross-border, and that limits on where data can be stored and processed are minimized, thereby enhancing and protecting the global digital ecosystem.*" With respect to the financial services sector specifically, the USMCA includes "*[u]pdated provisions to allow for the cross-border transfer of data and an updated market access obligation.*"
- Singapore-US Joint Statement on Financial Services Data Connectivity[20]: Among other things, "*[t]he United States and Singapore recognize that the ability to aggregate, store, process, and transmit data across borders is critical to financial sector development*" and agree to both oppose data localisation requirements and ensure "*financial service suppliers can transfer data, including personal information, across borders by electronic means if this activity is for the conduct of the business of a financial service supplier.*"
- Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas (BSP) and The Monetary Authority of Singapore[21]: BSP and MAS recognise that the ability to aggregate, store, process, and transmit data across borders is critical to the development of the financial sector.
- Singapore Digital Economy Agreements[22]: Singapore has executed a Digital Economy Partnership Agreement (DEPA) with Chile and New Zealand and a Singapore-Australia Digital Economy Agreement (SADEA) with Australia. Singapore is currently negotiating a Digital Economy Agreement with Korea and the UK. According to Singapore's Ministry of Trade and Industry, both DEPA and SADEA include provisions "*to allow data to flow freely across borders and prohibit the localisation of data except for legitimate purposes such as personal data protection*".

Principle 8: Approval and notification requirements

Regulators should not require pre-notification or approval for material public cloud arrangements. Rather, a regulated entity that commences a material cloud arrangement should keep an inventory of the arrangements that should be available to the regulator upon request.

[18] US Treasury (2019): Agreement between the Unites States of America and Japan concerning digital trade https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf

[19] US Treasury: US-Mexico-Canada trade fact sheet https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing

[20] MAS (2020): US-Singapore Joint Statement on Financial Services Data Connectivity https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

[21] MAS (2020) Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and the Monetary Authority of Singapore Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore (mas.gov.sg)

[22] Ministry of Trade and Industry Singapore Digital Economy Agreements (mti.gov.sg)

If regulators are not content with this proposal a regulated entity that commences a material public cloud arrangement should notify its regulator of the arrangement as soon as possible thereafter.[23] We recommend that any such notifications should be on a platform (critical systems/infrastructure) basis rather than based on specific applications (e.g., SaaS applications, deployments to IaaS environments).

If any pre-notification requirements are truly deemed necessary, we recommend that regulators adopt a streamlined, pragmatic and transparent notification procedure with reasonable timelines that provides certainty to the industry. Regulators should also provide flexibility and allow such notifications to be made at a higher level, such as for an overall system platform development plan or a cloud migration plan; and in case any additional notifications are considered necessary throughout the plan, FIs and regulators can work together early to identify and focus their attention only on the critical components of the plan.

We strongly discourage a need for formal approval as it creates additional bureaucracy for all parties, without clear value-add to the regulator in exercising its supervision responsibilities.

Principle 9: Concentration risk

In respect of the potential systemic risks arising from the concentration of third-party services, it is important to differentiate between the concentration risks that may exist where multiple regulated FIs use a common CSP (sector-wide concentration risks) and instances where a group is dependent on a single CSP for the provision of outsourced tasks (internal dependency).

- **Sector-wide concentration risk**: We believe that assessment of concentration risk in the sector should be done by authorities in close partnership with the financial services industry. For risks of this nature, authorities (e.g., supervisory bodies) are well positioned to have oversight at an industry level, as compared to FIs individually due to lack of visibility of which CSPs are used by other FIs. We believe, however, that any such assessment should not restrict the choice of outsourcing arrangements or providers available to FIs. The focus should be on operational resilience and reducing the risks arising from e.g. the impact of a disaster or insolvency event, rather than reducing concentration itself, which we believe would be difficult and require undesirable sacrifices to security, efficiency and innovation. In seeking to mitigate systemic risk, it is important that authorities avoid placing additional complexity or restrictions on an FI's ability to make commercial decisions and adapt to emerging business models and technologies, as some solutions to address industry-wide concentration risk currently proposed by authorities24 (e.g., exposure limits, rotation mechanisms) may limit the FI's ability to make commercial decisions and adapt to emerging business models and technologies.
- **Internal dependency:** In terms of an assessment of possible concentration risks within a firm caused by multiple cloud outsourcing arrangements with the same CSP, we recommend that firms should be able to undertake this as an internal assessment, based on risk appetite, and not be

[23] ASIFMA (2018): Proposed Leading Principles for Regulation of Outsourcing https://www.asifma.org/wp-content/uploads/2018/07/leading-principles-for-regulation-of-outsourcing.pdf.

[24] E.g. European Commission (2020): Draft regulation on Digital Operational Resilience for the financial sector https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

mandated to assess this on stipulated metrics that are set in regulatory guidance. Such an approach could affect the ability of a regulated FI to manage its oversight obligations and continuously enhance its resilience capabilities. Individual FIs can and should be able to practice their incident and risk management in this area.

- **Exit Plans:** We caution against the imposition of prescriptive obligations on FIs in order to mitigate concentration risks, and we maintain that FIs should have the freedom to select their third-party service providers and not be mandated by regulations to exit or duplicate their outsourcing arrangements or third-party services. While exit plans are feasible in the event of a medium to long term migration away from a CSP in a controlled and planned manner, they should not be used to address concentration risks. This is because such attempts at migrating the service could result in further operational risks such as mass migrations from a service which may destabilise markets, creating a potential for cascading outages. Emphasis on exit planning shifts the focus from resilience to replacement, when transitioning services during a business disruption may expose the FI and its customers to greater risk than ensuring effective recovery of services. Exit plans should be a last resort. Regulators should also weigh the concentration risk in relation to moving to cloud storage versus the risk of the alternative, which is using the FI's own data centres. Engineering, cyber and architectural best practices of CSPs often exceed on-premise capabilities and regulators should recognise that CSPs offer solutions to improve security, operational resilience and portability for FIs.