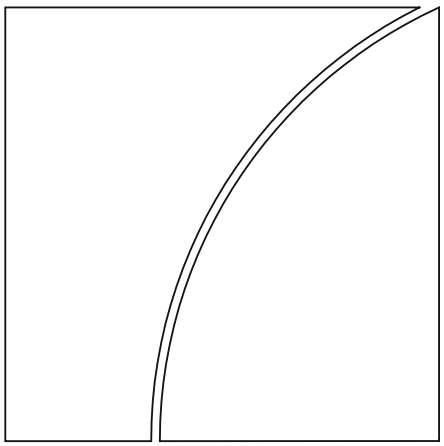
Financial Stability Institute

FSI Insights

on policy implementation

No 53



Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector

By Ting Yang Koh and Jermy Prenio

November 2023

JEL classification: G20, G28, O38
Keywords: cloud service provider, critical CSP

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Global Media and Public Relations team, please email media@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-249X (online)
ISBN 978-92-9259-706-1 (online)

Contents

Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector[1]

Executive summary

Financial firms' use of the cloud has been increasing over the years and is expected to continue to do so. The move to the cloud has accelerated especially during the past few years as companies bring forward their long-term digital transformation and modernisation initiatives after the pandemic. In the case of financial firms, there appears to be a significant increase in the critical workloads they have moved to the cloud, albeit these remain at a relatively low level.

The use of the cloud by financial firms presents benefits and risks. Cloud services allow easier access to infrastructure and services that would otherwise be expensive or take a long time to build and great cost to maintain, thus reducing the cost of financial services. Large cloud service providers (CSPs) can offer an IT environment that is relatively as robust as those that individual financial firms could create on their premises. However, cloud adoption introduces new risks that have the potential to affect financial firms' business operations. These risks include threats to data security and privacy, system availability, continuity of operations, interoperability, auditability and compliance with legal requirements.

The predominance of a small number of CSPs exacerbates these risks. Three players dominate the global cloud market and are also frequently used by financial firms across different jurisdictions. There may also be regionally or domestically significant CSPs used by financial firms. As such, the business continuity of many financial firms may be affected by cyber attacks and outages at any of these CSPs. This has been a significant concern in recent years, as demonstrated by recent global CSP outages. The risk is more pronounced and concerning for regulators if financial firms' critical functions reside within the same CSP.

Regulatory interventions are needed to address the risks arising from cloud adoption. Typically, control responsibilities are allocated between the CSP and the entity acquiring its services. Financial firms that use the cloud have a responsibility to ensure the availability, resiliency and security of the services they provide to their customers in the cloud, while CSPs need to take steps to make the overall environment resilient and secure. However, financial firms might not have full visibility into the risk management and control measures adopted by CSPs. In addition, while financial firms have measures at their disposal to ensure the availability and resilience of their cloud workloads, such as the adoption of a multi-zone and multi-cloud approach, such measures can lead to increased cost, complexity and resource demands to design and operate in different cloud environments. As such, financial firms alone do not have the ability to fully mitigate risks arising from cloud adoption.

In some jurisdictions, CSPs are subject to horizontal or cross-sectoral regulations. These may include requirements to register or apply for a licence as well as meet other requirements imposed by information and communications technology (ICT) authorities. They also include cyber security regulations issued by cyber security authorities that cover a wide range of industries. Other jurisdictions also have laws or regulations in place imposing requirements on their critical infrastructure, including data storage and processing.

[1] Jermy Prenio (Jermy.Prenio@bis.org), Bank for International Settlements; and Ting Yang Koh (Koh_Tingyang@mas.gov.sg), Monetary Authority of Singapore. We are grateful to Boris Petru Augustinov, Chester Chua, Mel Grantham, Markus Grimpe, Stefan Hohl, Mattias Levin, Orlando Fernández Ruiz, Maria Tsani, Michalis Tsavdaridis and participants of the breakout session on "Regulating critical cloud service providers" at the Consultative Group on Risk Management for the Americas' Cloud Security and Resilience Workshop (24 August 2023) for helpful comments and insights. Anna Henzmann provided valuable administrative support.

In the financial sector, the prevalent approach is an indirect oversight of CSPs, which may not be sufficient from a systemic perspective. This approach mainly relies on financial firms to manage the risks that arise from acquiring third-party services and to assess the potential implications of such services for their own operational resilience. This approach does not really address financial firms' limitations when it comes to assessing and addressing the CSP risks mentioned above. Moreover, while this approach may potentially address risks faced by individual firms, it may not be sufficient to address the potential impact on the financial system of an operational disruption of a CSP. A few jurisdictions therefore have or are planning to have a more direct oversight approach to CSPs that are considered critical to the functioning of the financial system. There is also interest among many jurisdictions in exploring this possibility.

This paper identifies some considerations for financial authorities when introducing direct oversight frameworks for critical CSPs. First, financial authorities may want to leverage existing cross-sectoral regulations issued by ICT and cyber security authorities. Where there are already national critical infrastructure regulations or laws in place, financial authorities' direct oversight intervention should be consistent with this approach. Second, it is important to closely coordinate with relevant non-financial authorities because they bring relevant expertise to the table. Close coordination in the design and enforcement of relevant requirements for CSPs by various authorities could help ensure alignment of regulatory requirements and expectations, as well as reduce inefficiencies when engaging with CSPs. More importantly, this close coordination should result in an efficient and effective flow of information as well as response and recovery measures in the event that a critical CSP experiences a systemic operational disruption.

Financial authorities' strategies may differ depending on their legal mandates. If they have legal mandates to directly regulate CSPs, they may consider introducing additional requirements for critical CSPs on top of the horizontal regulations, taking into account financial sector-specific concerns. These requirements may include higher risk management or resilience standards, or more frequent and intensive resilience testing and incident response and recovery exercises. To avoid moral hazard (ie financial firms passing their responsibility and accountability for managing third-party risk to the financial authorities), the introduction of these direct requirements should not eliminate the obligations of financial firms under the indirect oversight approach. If financial authorities have no legal mandates to oversee CSPs and there are no relevant horizontal authorities in their jurisdictions, financial authorities need to strengthen the existing indirect oversight approach. They could, for example, strengthen requirements for financial firms using critical CSPs, with the expectation that these requirements would be reflected in the firms' arrangements with the CSPs.

Cross-border arrangements for the oversight of a critical CSP are necessary. This is especially the case where a CSP is considered critical in multiple jurisdictions and there are no restrictions on the CSP's use of data centres outside of these jurisdictions. Under such conditions, operational disruption of the CSP may have cross-border impacts. Having cross-border oversight arrangements will also ensure that critical CSPs are subject to consistent regulations and standards across jurisdictions and will avoid unnecessary duplication of regulatory work. But the first step is to identify CSPs that may be critical in multiple jurisdictions. Here, global standard-setting bodies could play a role.

Cross-border oversight arrangements can be informal or formal. Informal arrangements are voluntary groups that share information or best practices. They can also be used as a platform to undertake ad hoc joint resilience testing or exercises. Formal arrangements could take the form of a collective cross-border oversight body for a specific CSP. The organisation of this body could be inspired by the regime put in place for facilities with cross-border importance or by supervisory colleges. Formal arrangements can facilitate the same activities as informal arrangements, but the former would be able to put in place binding measures that are preventative and corrective. In either case, as at the national level, one of the objectives of these arrangements should be to ensure the ability to respond efficiently and effectively in the event of a cross-border and systemic incident involving a CSP or CSPs.

Section 1 – Introduction

1. **Financial firms' increased reliance on technology and technology providers such as cloud service providers (CSPs) highlights the need for financial authorities to better manage operational resilience issues at the financial system level.** In recent years, new technologies are increasingly being used by financial firms. Some of these technologies are provided as an outsourced service by technology companies. Cloud service is one example. In general, the use of cloud by a typical financial firm can enhance its IT security beyond what the firm alone can accomplish. However, given that the provision of cloud services is largely concentrated in a few global technology companies, the consequences for the financial ecosystem of an operational disruption of a CSP could be quite severe, especially if financial firms' critical functions are in the cloud. The potential impact could also be cross-border and cross-sectoral given the extensive business reach of the few leading CSPs. Financial authorities therefore may see the need to assess and manage the likely impact of these potential disruptions on operational resilience beyond the individual financial firm level.

2. **The prevalent regulatory approach to the use of CSPs by financial firms may not be enough from a systemic perspective.** The most common regulatory approach focuses on how financial firms manage their own risks arising from acquiring third-party services, including that of CSPs. Regulations typically require financial firms to assess the potential implications of such services for their own operational resilience. This includes performing due diligence in selecting service providers, as well as making sure that contractual agreements provide financial firms the right to inspect or audit their service providers (sometimes including their significant subcontractors). This approach addresses microprudential concerns, but may not be sufficient from a macroprudential perspective considering the potential implications of an operational disruption of a CSP outlined above. In addition, the market power that the leading CSPs have raises the question of whether financial firms have the right competency, powers and means to perform thorough assessments of risks as envisaged in existing regulations. This led Prenio and Restoy (2022) to argue that there may be a case for subjecting CSPs, particularly those critical for the financial system, to an oversight framework.

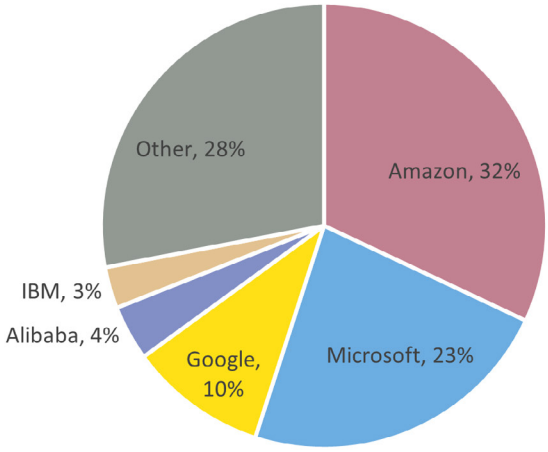
3. **The importance of identifying, monitoring and managing potential systemic risks from third-party dependencies has been explicitly acknowledged by the Financial Stability Board (FSB).** FSB (2023) recognises that individual financial firms may be unable to adequately manage these systemic risks. It alludes to financial authorities in some jurisdictions having or being in the process of acquiring regulatory powers over critical service providers, but also notes that financial authorities in other jurisdictions do not have the legal powers to do so. As such, it proposes some tools to help financial authorities identify systemic third-party dependencies and spot and manage potential systemic risks. This paper builds on FSB (2023) by (i) focusing on critical CSPs and (ii) identifying considerations in the oversight of such critical CSPs by financial authorities.

4. **This paper explores what potential oversight frameworks for critical CSPs might look like, taking into account the cross-border and cross-sectoral nature of their operations.** Section 2 provides background on the use of cloud services in the financial sector. Section 3 outlines the existing prevalent regulatory approach. Section 4 discusses existing or proposed regulations or oversight practices directly applicable to CSPs. Section 5 explores considerations when enhancing or introducing regulations or oversight practices to better manage the far-reaching impact of a potential operational disruption of a critical CSP. Section 6 concludes.

Section 2 – Background on cloud services and their use in the financial sector

5. **The FSB defines cloud computing as an innovation that allows for the use of an online network of hosting processors to increase the scale and flexibility of computing capacity.** There are different types of cloud computing service model (Infrastructure as a Service, Platform as a Service, Software as a Service and Business Process as a Service), as well as different types of deployment model (public cloud, private cloud and hybrid cloud).[2] It is worth noting that three CSPs – Amazon Web Services, Microsoft Azure and Google Cloud – dominate the global cloud market, accounting for almost two thirds of the market (Graph 1).

Market share of CSPs — Graph 1



Source: Synergy Research Group.

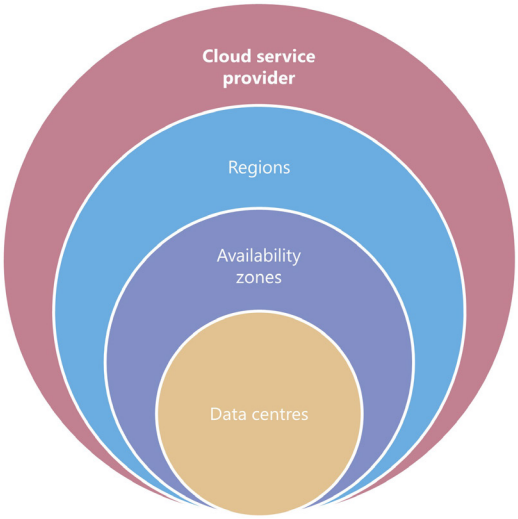
6. **CSPs are generally organised into regions and availability zones.** These are meant to improve resilience and reduce latency.[3] These discrete areas also determine disaster recovery and data residency boundaries. In addition to regions and zones, CSPs also have a network of "points of presence", communication devices strategically located near end users in order to connect to data centres to further reduce latency and improve the performance of applications. Box 1 illustrates how CSPs are generally organised and defines the different components, while the Annex shows jurisdictions with CSP regions. It is worth noting that only 36 jurisdictions host regions of the top three global CSPs, ie their data centres are located in these jurisdictions. This means that customers in jurisdictions not on the list are dependent on CSP data centres located outside their jurisdictions. Customers adopting a multi-region strategy (see below for more discussion on this) may also depend on data centres located abroad.

[2] See FSB (2019) for an explanation of these different types of cloud service and deployment model.

[3] Resilience refers to the reduction in the risk of a single point of failure, while latency refers to lag in network communication.

Box 1

How are CSPs generally organised?



CSPs are generally organised across three layers to ensure the availability and resilience of their services:

- **Data centre** – a physical facility that houses actual servers, storage and networking equipment etc; each data centre is designed to remain operational in the event of a failure in other data centres.
- **Availability zone (AZ)** – a group of closely located data centres; since data centres in the same AZ are in the same general area, they are exposed to the same physical risks, such as natural disasters or power failure. As such, an AZ is considered a single failure domain.
- **Region** – a group of AZs within a geographical area; all AZs within a region, while fully independent, are interconnected via dedicated high-bandwidth, low-latency links; similarly, while all regions are isolated for fault tolerance, they are interconnected in the same way that AZs in the same region are.

Financial firms can host or replicate workloads in multiple AZs or even regions. These multiple deployments help with business continuity and data recovery, minimising the risk of a single point of failure.

Source: Dgtl Infra; illustration by authors.

7. **Institutions that use public cloud have a role to play in securing their cloud workloads.**[4] It is common practice to allocate control responsibilities between the cloud service provider and their customers. This is referred to as the "shared responsibility" model. Customers are responsible for maintaining a secure control environment within the cloud. This involves the administration, security and resilience of cloud workloads, applications, operating systems, virtual networks and data, which can be managed differently from traditional on-premises IT infrastructure risks due to the unique characteristics of public cloud services. For example, in the Infrastructure as a Service (IaaS) model, it is the customer's responsibility to ensure the security of the operating system, applications and data hosted on the infrastructure. This includes configuring firewall rules, applying security patches and managing user access controls. On the other hand, it is the CSP's responsibility to secure the underlying infrastructure, including servers, storage, networking and data centres. Customers will be dependent on cloud service providers for security **of** the cloud, such as ensuring the timely patching of services and devices on the provider's end. Meanwhile, customers are directly responsible for security **in** the cloud, which includes configuring their

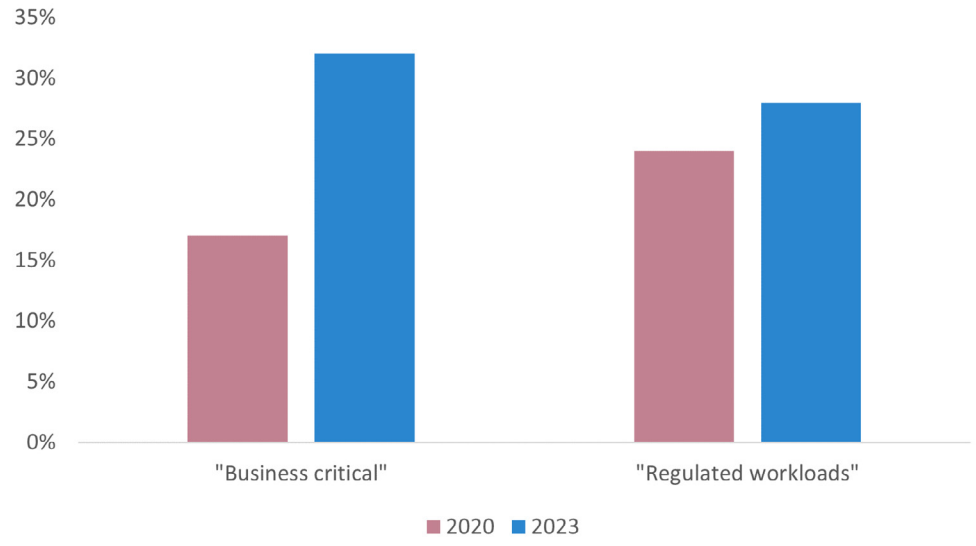
[4] A cloud workload is a virtualised instance of a specific application code or service that can be run on a cloud resource and supports a defined process. This may include virtual machines, databases, containers and applications.

cloud environments in a secure manner. Nonetheless, customers might not have complete visibility into the risk management and control measures adopted by CSPs.[5]

8. **Public cloud adoption is increasing across all industries.** According to Gartner (2022), enterprise IT spending on public cloud computing will overtake spending on traditional IT in 2025. The shift to the cloud has accelerated especially during the past few years due to the Covid-19 pandemic. The increasing need for integration capabilities, agile work processes and composable architecture is expected to further accelerate the shift to the cloud as companies bring forward their long-term digital transformation and modernisation initiatives after the pandemic.

9. **Financial firms in particular have made increasing use of cloud computing in recent years.** A 2021 survey conducted by Google Cloud, together with the Harris Poll,[6] revealed that 83% of the 1,300 financial firms surveyed globally are already using some form of public cloud, including hybrid and multi-cloud approaches.[7] The digital footprints of financial firms in the cloud are expected to grow further; among those without an existing cloud deployment, 88% are considering adopting a cloud strategy in the next 12 months. In the last few years, for example, there has been a significant increase in the number of financial firms moving their workloads designated as "business critical" to the cloud. Financial firms have also moved "regulated data" to the cloud, albeit at a slower pace (Graph 2).[8]

Cloud adoption in certain areas of financial firms — Graph 2



Source: CSA.

10. **The use of cloud services provides benefits to financial firms.** Cloud services allow easier access to infrastructure that would otherwise be expensive or take a long time to build and great cost to maintain, thus reducing the cost of financial services. Economies of scale allow CSPs to achieve a high degree of redundancy, geographic diversity and advanced security and engineering at a much lower cost. Large CSPs in particular can offer an IT environment that is more or at least as robust as those that individual financial firms could create on their premises.

[5] See US Department of the Treasury (2023).

[6] See Google (2021).

[7] A multi-cloud approach refers to the use of services from different CSPs.

[8] See CSA (2023). The report does not define "business critical" and "regulated data".

11. **However, aside from traditional outsourcing risks, cloud computing may pose additional operational and reputational risks to financial firms.** The adoption of cloud computing technology by financial firms introduces operational and reputational risks that have the potential to impact their business operations. These risks include threats to data security and privacy, system availability, continuity of operations, interoperability, auditability and compliance with legal requirements. The impact of these risks may vary depending on factors such as the service model used; the type of IT assets being stored, processed and transmitted; and the unique usage of cloud technology within the firm's business operations.[9]

12. **The predominance of a small number of global CSPs could lead to systemic risk.** As mentioned, three players dominate the global cloud market across industries. These dominant global players are also frequently used by financial firms across different jurisdictions. Moreover, there may be regionally or domestically significant CSPs used by financial firms.[10] As such, the business continuity of many financial firms may be affected by cyber attacks and outages at any of these CSPs. This has been a significant concern in recent years. For instance, the two global outages that Microsoft's cloud services Azure, Teams and Outlook[11] experienced within a short span between January and February 2023 exemplified the widespread disruption and impact such outages can have on clients, including financial firms. The risk is more pronounced and concerning for regulators if many critical systems are residing within the same CSP.

13. **Besides securing the control environment within the cloud, it is important for financial firms to put in place strategies to ensure the availability and resilience of their workloads in the public cloud.** For cloud workloads that require high availability, firms should ensure that the appropriate cloud redundancy or fault-tolerant features offered by CSPs are enabled. To mitigate any location-specific issues that may disrupt the delivery of public cloud services, firms can consider deploying their cloud workloads across multiple zones or regions (see discussion above). Firms may also consider implementing vendor diversity measures such as a multi-cloud strategy, which involves using multiple cloud service providers to meet an organisation's needs.[12]

14. **There are drawbacks to adopting a multi-zone and multi-cloud approach.** These include increased cost, latency and the potential absence of comparable services across different regions of the same CSP. Additionally, implementing a multi-cloud strategy can present further challenges and new risks due to inherent differences among service offerings and increased complexity and resource demands to design and operate in different cloud environments. As a result, it will be challenging for financial firms to design applications and data for portability to another CSP for many complex services or to address operational continuity in the short term.[13] These challenges could explain why the number of financial firms that are using multiple CSPs has gone down in recent years (Graph 3, left-hand panel). More concerning is the increase in the number of financial firms without a documented backup plan should their subscribed cloud services be disrupted. Of those that have a documented plan, many are untested (Graph 3, right-hand panel).

[9] See Crisanto et al (2018).

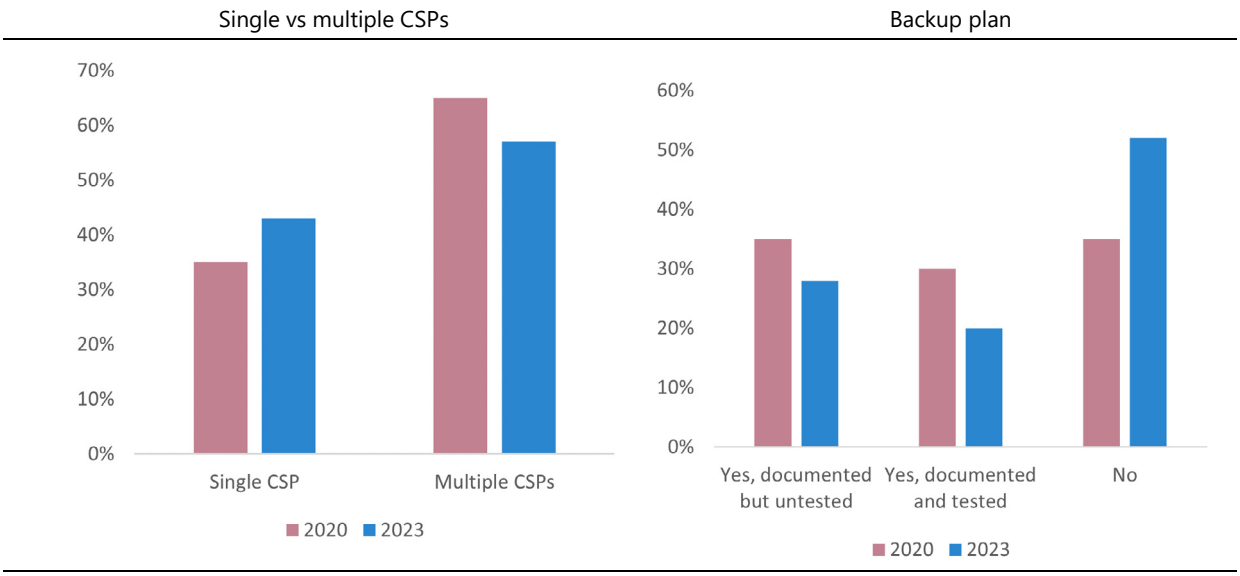
[10] See FSB (2019).

[11] See Stone Forest Business Advisors (2023).

[12] See BOJ (2021) and MAS (2021).

[13] See US Department of the Treasury (2023).

Cloud strategy and business continuity of financial firms Graph 3



Source: CSA.

Section 3 – The existing prevalent approach: indirect oversight of CSPs used in the financial sector[14]

15. **The regulatory principle that applies to the use of third-party services in the financial sector typically leads to an indirect approach by financial authorities regarding the oversight of CSPs.** This principle refers to the ultimate accountability of a financial firm's board and senior management for any activities, functions, products or services that they outsource to a third party. Hence, financial authorities rely primarily on financial firms to manage the risks arising from third-party services. This is reflected in the regulatory requirements and supervisory expectations regarding how firms should oversee third-party relationships. The regulatory and supervisory focus is on the assessment of the adequacy of financial firms' outsourcing and contractual frameworks. Moreover, most jurisdictions also require financial firms to notify or seek authorisation from financial authorities before hiring material third-party services, including cloud services.

16. **Regulations typically require financial firms' outsourcing frameworks to define the governance and risk management surrounding activities or functions that are delegated to third parties.** Financial firms' board-approved outsourcing frameworks are typically required to define the applicable roles and responsibilities within the financial firm, the activities and functions that can be outsourced to third parties, the conditions for outsourcing and the specific risks that need to be analysed and managed. Risks that financial firms need to analyse and manage when dealing with third parties include strategic risk, compliance risk, security risk (including cyber security), counterparty risk, business continuity risk, vendor lock-in risk, contractual risk, concentration risk[15] and, where relevant, country risk.

[14] Based mainly on BCBS (2018) and FSB (2020).

[15] In this context, concentration risk refers to a firm's reliance on a single third party for multiple activities or functions.

Outsourcing frameworks are also commonly expected to provide for the maintenance of an inventory of outsourced activities or functions.

17. **In terms of contractual frameworks, regulations commonly require these to define the generic rights, obligations, roles and responsibilities of the institutions and the third-party service provider.** It is common for regulations to explicitly require contractual terms to include confidentiality agreement and security requirements for safeguarding firms' and customers' information. In jurisdictions with contractual framework requirements that deal specifically with cloud services, information transferred to the cloud is typically expected to be subject to a security and confidentiality clause in the contract. Some jurisdictions also have specific requirements regarding data location, data segregation and data use limitations. Many regulations also require that contracts guarantee financial firms' rights to inspect and audit their third-party service providers. Some jurisdictions grant these rights directly to financial authorities. This is the case, for example, in Australia, where the Australian Prudential Regulation Authority's (APRA) Prudential Standard CPS 230 provides that material service provider agreements must include the right for APRA to access documentation, data and any other information related to the provision of the service; allow APRA the right to conduct on-site visits to the service provider (may be a third party, related party or connected entity); and ensure the service provider agrees not to impede APRA in fulfilling its role. There are also supervisory expectations about financial firms receiving regular reports from third-party service providers on measurements of service level agreements and the performance of controls.

18. **Many financial authorities also expect financial firms to have an assurance process regarding the operational resilience of third parties, but there are implementation challenges.** At the international level, BCBS (2021) requires banks to verify that third parties have at least an equivalent level of operational resilience in order to safeguard the bank's critical operations in both normal circumstances and in the event of disruption. However, financial firms, particularly smaller ones, may not have the capacity to undertake this assurance process. Some regulations therefore encourage an industry solution if there are synergies across assurance work by firms on third parties, such as through certifications. Similarly, recognising the challenges of auditing large third-party technology providers, some authorities now accept pooled audits (ie audits done collaboratively with other financial firms that are also clients of the third party) or independent audits performed on the third party by either its internal audit function or an external auditor. In addition, some authorities acknowledge that in some cases it may not be appropriate to carry out sophisticated testing on large third-party providers. If this is the case, firms should seek alternative ways to gain assurance of their operational resilience, such as desktop testing.[16]

Section 4 – Regulations/guidance/supervisory/oversight practices directly applicable to CSPs

19. **There are already existing approaches for direct oversight of CSPs.** Many of these approaches apply across different sectors, while recent approaches are specific to the financial sector. It is important to note that this paper focuses on resilience-related laws and regulations. There may be other laws and regulations pertinent to CSPs, such as data protection, that are also crucial in overseeing their operations, but these are not specifically included in the discussions below unless part of an overall framework.

[16] See BoE/FCA (2021).

With cross-sectoral application

20. **Some jurisdictions have regulatory frameworks that are specifically applicable to CSPs.** In Saudi Arabia and Malaysia, for example, CSPs are required to register or apply for a licence to provide cloud computing services.

- **In Saudi Arabia, the regulatory framework established by the Communication, Space and Technology Commission (CST)[17] serves to promote safe and secure use of cloud computing services in the country and provide the appropriate regulatory environment to attract local and international CSPs.** The framework applies to cloud computing services provided to customers residing in or having an address in Saudi Arabia. It requires CSPs with direct or effective control of data centres or critical infrastructures of cloud computing systems hosted and used in the country to register with the CST.[18] The registration requirements are based on the type of data that the CSP will be hosting and processing, in accordance with the data classification. This gives CSPs the clarity and flexibility to fulfil the requirements of their targeted subscribers. The framework's provisions are designed to guarantee that CSPs adhere to best practices and technical standards. These encompass aspects such as service quality, contractual relationship and protection of both service providers and users. For instance, CSPs must guarantee the implementation of robust rules and policies pertaining to business continuity and risk management, in addition to informing their subscribers about the status of the service level agreement and whether it is being fulfilled or not.
- **CSPs in Malaysia are regulated by the Malaysian Communications and Multimedia Commission (MCMC) as provided under the Communications and Multimedia Act (CMA) 1998.[19]** Cloud services fall under "class licence" for application services under CMA 1998. Class licence only requires registration, which is an administrative process and hence a light-touch regulation designed to promote industry growth and development.[20] The licence is imposed only on CSPs that are locally incorporated, or on CSPs that are not locally incorporated but provide cloud services to end users through a local data centre, in which case the local data centre is required to be licensed.

21. **Other jurisdictions are actively developing new regulatory frameworks for CSPs.** In Vietnam, the government is working on a new draft telecoms law that would require cloud service providers to also obtain a telecoms licence and establish a legal presence in Vietnam. This is in addition to existing laws on information technology and cyber security that are also applicable to cloud services.[21] Singapore is currently exploring amending the existing Cybersecurity Act to ensure the cyber security of foundational digital infrastructure, which is expected to include cloud services.[22]

22. **Authorities in some jurisdictions have issued guidance to support adoption of cloud services across government and industry.** Authorities that follow this approach include the Australian Cyber Security Centre (ACSC) and Australia's Digital Transformation Agency (DTA) and Hong Kong SAR's Office of the Government Chief Information Officer (OGCIO). In Australia, ACSC and DTA, in collaboration with the industry, have issued cloud security guidance that aims to support the secure adoption of cloud

17 See CST (2023).

18 This does not preclude CSPs from using data centres located outside Saudi Arabia to process, store, transport or transfer the data of customers who reside or have an address in the country (unless these are government data). However, the CST has the right to refuse the use of data centres located outside its jurisdiction.

19 See MCMC (2021).

20 See MCMC (2017).

21 See Vietnam Business Law (2023).

22 See Cyber Security Agency of Singapore (2022) and MCI (2023).

computing across government and industry. The guidance helps assessors validate CSPs' security posture, thus providing organisations with independent assurance. In the case of Hong Kong, its OGCIO has issued a *Practice guide for cloud computing security* to provide practical guidance and reference for the secure adoption of cloud computing technology in the government.[23]

23. **National authorities have also introduced laws or regulations on cyber security that encompass a wide range of industries and services including cloud computing services.** Notably, the EU's Network and Information Security (NIS) Directive, which came into effect in May 2018 and was updated in 2022, sets out measures to achieve a high common level of reliability and security of network and information systems in the Union and covers digital service providers (DSPs), such as CSPs, as well as operators of essential services (OES) (eg a bank or a financial market infrastructure could be designated as an OES). The NIS Directive defines different obligations across the EU, one of which concerns the establishment of one or more Computer Security Incident Response Teams (CSIRTs) at the national level for comprehensive incident management nationwide.[24] The United Kingdom also has its Network and Information Systems Regulations 2018, or NIS Regulations, which aim to ensure the security of network and information systems across various sectors and cover cloud services.[25] Australia's Security of Critical Infrastructure Act 2018 is another example. It is aimed at addressing national security risks associated with Australia's critical infrastructure (including that provided by foreign providers) and has been amended in 2021 and 2022 to apply to 11 economic sectors, including data storage and processing.[26]

Specific to the financial sector

24. **In the financial sector, direct oversight of third-party service providers is not new, but it has historically been done on a contractual or ad hoc basis.** As mentioned above, some regulations already require third-party contracts to grant financial authorities the right to inspect and audit third parties. However, this contractual means of gathering information may not be as effective as having statutory authority.[27] Some jurisdictions have laws that provide financial authorities with statutory powers to regulate and examine third-party services if they deem appropriate. This is the case for example in the United States, where federal banking agencies[28] may exercise this power under the Bank Service Company Act.[29] Exercise of this power is based on a case by case analysis of, among others, the criticality of the service, the number of financial institutions under contract with the service provider and the inherent risk that the service may present to client financial institutions. In addition, Title VIII of the Dodd-Frank Act allows supervisory agencies of designated financial market utilities (DFMUs)[30] to examine the provision of a service provided by another entity when such a service is "integral" to the operation of the DFMU.[31]

23 See OGCIO (2021).

24 See BCBS (2018).

25 The United Kingdom's NIS Regulations transposed the EU's 2018 NIS Directive before the United Kingdom's departure from the EU. The UK government has consulted on amendments to the NIS Regulations and plans to update them in due course. See more from UK Government, "Government response on amending the NIS regulations", 17 November 2021.

26 See US Department of the Treasury (2023) for a comparison of international regulatory approaches in the use of cloud services in the financial sector.

27 Ibid.

28 Namely the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency.

29 This power does not extend to services provided to entities not covered under the BSCA or to the service provider more generally.

30 Namely the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission and the Commodity Futures Trading Commission.

31 See US Department of the Treasury (2023).

25. **At the international level, the Principles for Financial Market Infrastructures (PFMI) of the BIS Committee on Payments and Market Infrastructures (BIS CPMI) and the International Organization of Securities Commissions (IOSCO) have already set out expectations applicable to critical service providers.** Annex F of the PFMI describes these expectations. These include expectations related to risk identification and management, information security, reliability and resilience, technology planning and communication with users. While these expectations are targeted specifically to critical service providers of FMIs, they may also serve as a template for critical service providers of financial firms. For example, Annex F of the PFMI forms the basis of the requirements for critical service providers of recognised payment system operators in the United Kingdom, which are under the direct oversight of the Bank of England.

26. **Recent developments at the national or regional levels have explicitly recognised the potential systemic risks from third parties and introduced or proposed comprehensive direct oversight frameworks.** This is the case with the Digital Operational Resilience Act (DORA) in the EU and the proposed framework for critical third parties (CTPs) in the UK financial sector, which covers CSPs.[32] Both frameworks point to the systemic risks that arise from financial firms' increasing reliance for critical services on certain third parties, which are highly concentrated and whose services are often very difficult or impossible to substitute in case of disruption. In the case of the EU, this motivated the need to have a framework that would allow for continuous monitoring of the activities of critical ICT third-party service providers. In the case of the United Kingdom, this led to the realisation that additional policy measures are needed to mitigate the financial stability risks arising from concentration in third-party service providers, as a complement to the requirements and expectations for individual financial firms regarding operational resilience and third-party risk management.

27. **Elements of DORA and the UK proposal are quite similar.** DORA and the UK proposal have not yet been implemented. The relevant authorities in the EU are still fleshing out specific regulatory technical standards, while those in the United Kingdom are still developing certain detailed elements of the policy as well as their future approach to oversight of CTPs. Consequently, Table 1 and the following paragraphs capture the EU and United Kingdom's respective current, publicly known policy positions, which are likely to evolve.

Main elements of the EU's DORA and the UK proposal on CTPs — Table 1

	DORA	UK proposal
Designation criteria for CTPs	Criticality/materiality of the service provided or the type of financial firms' functions that rely on the service.	Criticality/materiality of the service provided or the type of financial firms' functions that rely on the service.
	Concentration or the number and type of financial firms (including their systemic significance) relying on the service provider.	Concentration or the number and the type of financial firms (including their systemic significance) relying on the service provider.
Authorities involved	Lead overseer depends on the type of financial firms that mainly rely on the service provider: EBA; ESMA; EIOPA.	Bank of England/Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA).
	An oversight forum supports the lead overseer.	

[32] See EU (2022) and BoE/FCA (2022).

Subject of oversight	Designated CTPs should establish a subsidiary in the EU.	No requirement to establish a local subsidiary. Only focus on services that the CTP provides to financial firms and not on the entire entity and operations of the CTP.
Standards to which CTPs will be subject	No explicit set of standards, but CTPs will be assessed on how they manage ICT risks.	Considering a set of resilience standards inspired by Annex F of the PFMI and other relevant global standards, but tailored to CTPs in the financial sector as a whole.
Supervisory powers	Lead overseer can recommend measures to CTPs and impose penalties if they refuse to collaborate.	Relevant authority can require CTPs to do or refrain from doing certain actions and can publish a statement/impose conditions/disqualify if they refuse to comply.
Cross-sectoral coordination	Digital service providers (DSPs) in the NIS Directive could also be subject to DORA oversight, but this is on a case by case basis.	Potential coordination with non-financial authorities in relation to designation of CTPs, resilience standards, testing and incident reporting.
Cross-border cooperation	Envisaged in relation to developing best practices for the review of ICT risk management practices, controls, mitigation measures and incident responses.	Potential areas include global methodology for identification of CTPs, global resilience standards and cross-border resilience testing.

Source: FSI analysis.

28. **In terms of designation, in essence both frameworks focus on potential impact based on criticality/materiality and concentration.** Criticality/materiality does not refer only to the service provided by the third party (ie whether disruption to the service would result in large-scale operational failure); it also refers to the type of financial firm to which the third party is providing services (ie systemically important financial institution or not) and the functions of the firm that rely on the third-party service (ie whether they are considered essential functions to the economy or not). Concentration refers to the number of financial firms to which the third party provides services. This also includes the degree of substitutability of the third-party service provider.

29. **Both frameworks envisage coordination among relevant financial authorities, and there could be a lead authority.** In the EU, any of the three European Supervisory Authorities (ESAs) – ie the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) – could be designated as a "Lead Overseer", depending on the type of financial firms that mainly rely on the service provider. There is also an oversight forum that supports the work of the lead overseer. The oversight forum will carry out preparatory work both for the individual decisions addressed to critical CTPs and for issuing collective recommendations, in particular in relation to benchmarking the oversight programmes for critical CTPs and identifying best practices for addressing CTP concentration risk issues. The United Kingdom is still developing its approach on this issue, but the legislation granting the Bank of England, the PRA and the FCA powers over CTPs requires them to coordinate the exercise of their respective functions regarding CTPs. The discussion paper published in 2022 was issued jointly by the three authorities, which signals their intention to work collaboratively.

30. **The two frameworks have different approaches as to how CTPs should be subject to oversight.** In DORA, designated CTPs are required to establish a subsidiary in the EU. The rationale given was to ensure the enforceability of supervisory actions (see below) and "to allow a swift rollout of procedures upholding the critical ICT third-party service providers' rights of defence in the context of the

designation mechanism and the issuance of recommendations".[33] However, this requirement does not preclude CTPs from supplying services from facilities and infrastructure outside the EU. If such is the case, the lead overseer needs to be able to exercise its relevant oversight powers in third countries subject to the consent of the critical ICT third-party service provider. Relevant authorities of the third country should also be informed of – and not have objected to – such exercise of oversight powers in their territory. Such powers also need to be fully anchored in the conclusion of administrative cooperation arrangements with the relevant third-country authority/ies. In the UK proposed framework, there is no requirement for CTPs to put up a local subsidiary. In addition, the proposal emphasises that supervisory authorities would not oversee, regulate or supervise CTPs in their entirety, but would only "focus on those services that CTPs provide to firms and FMIs whose failure or disruption could have a systemic impact on the supervisory authorities' objectives".[34]

31. **While both frameworks would assess the operational resilience of CTPs, the UK proposed framework is more explicit as to the standards for this assessment.** UK authorities consider that a set of standards similar to those in Annex F of the PFMI, but applicable and tailored to CTPs in the financial sector as a whole, could be a key tool for managing the systemic risks that they pose. The UK proposal therefore includes potential minimum resilience standards in several areas, including identification of critical services and mapping of resources required to provide these services, risk management, testing, engagement with supervisory authorities, development of a financial sector continuity playbook, post-incident communication, and learning and evolving from severe disruption experiences. DORA is not as explicit in these requirements, but does specify that critical ICT third-party service providers will be assessed regarding whether they have in place, among others, comprehensive, sound and effective rules, procedures and mechanisms to manage ICT risks. The outcome of the assessments will inform the oversight plan and actions for each critical ICT third-party service provider.

32. **Both frameworks provide supervisory powers to relevant financial authorities.** In the case of DORA, the lead overseer can recommend measures to improve a CTP service provider's management of ICT risk. The lead overseer can impose penalties on the service provider for refusing to collaborate (eg not providing information and documents, refusal to submit to inspections and investigations, not providing reports on follow-up actions etc). In the case of the UK proposed framework, supervisory authorities can require a CTP to do or refrain from doing certain actions; appoint a skilled person to provide a report on the third party's compliance with relevant requirements; and, if a third party does not comply with a requirement, publish a statement or impose conditions or limitations on the ability to provide services and issue a disqualification notice.

33. **Both frameworks provide for cross-sectoral and cross-border cooperation and coordination.** DORA envisages cross-sectoral coordination for critical ICT third-party service providers that are supervised under the EU NIS Directive. The lead overseer should consult the competent authorities under that Directive in order to have a coordinated approach when dealing with the relevant critical ICT third-party service providers. The UK proposal, on the other hand, anticipates potential coordination with authorities outside the finance sector in relation to designation of CTPs, resilience standards, testing and incident reporting. In terms of international cooperation and coordination, DORA allows supervisory authorities to enter into administrative arrangements with third-country regulatory and supervisory authorities in order to develop best practices for the review of ICT risk management practices, controls, mitigation measures and incident responses. Similarly, the UK proposal lists potential ways to strengthen international coordination on CTPs, including on a global methodology for identification of such third parties, global resilience standards and cross-border resilience testing.

[33] EU (2022).

[34] BoE/FCA (2022).

Section 5 – Some considerations when enhancing or introducing direct oversight frameworks for critical CSPs to the financial sector

34. **As discussions above illustrate, the concern over critical CSPs to the financial sector arise from two sources: (i) potential impact and (ii) concentration.**[35] The potential impact depends on the criticality/materiality of the financial services that rely on the cloud. Concentration refers to the degree of financial firms' reliance on a few CSPs. An outage at a CSP could disrupt the delivery of critical/material services in the financial system. Such disruption could have an impact on financial stability. This impact is compounded if the CSP user is a systemically important financial institution or if the CSP is being used by many, if not most, financial firms. In the latter case, an outage at a CSP could lead to a virtual complete halt in the delivery of critical/material financial services.

35. **As such, any potential new or enhancements to oversight frameworks for critical CSPs need to address these concerns.** The indirect oversight approach, where financial firms manage their relationship with CSPs and the risks this poses to their individual operations, remains useful. This is particularly the case for financial authorities that do not have legal powers to oversee critical CSPs and are in jurisdictions without relevant authorities that directly oversee CSPs. In such cases, indirect oversight should be strengthened by, for example, enhancing requirements for financial firms using critical CSPs, with the expectation that these requirements would be reflected in the firms' arrangements with the CSPs. However, where feasible, it is equally important to have direct assurance or means for the financial authorities to ensure that financial stability concerns arising from the use of CSPs for the provision of services critical to the financial system are addressed.

36. **Financial authorities' direct oversight frameworks for critical CSPs can help address issues that may hinder financial firms' assessment of CSP risk.** These issues arise from the market power inherent in the dominant presence of a few CSPs, as well as the CSPs' clear advantage when it comes to technical skills. It is therefore uncertain whether financial firms would have the right incentives and the means to perform thorough assessments of CSP risks. Direct oversight frameworks can help address these issues and be a good complement to indirect oversight frameworks. Authorities, for example, would have more sway, either individually or collectively, in demanding that CSPs introduce changes to their security controls/processes to address risks that may be identified. However, there is a risk of moral hazard when introducing direct oversight frameworks. Financial firms will likely pass their responsibility and accountability for managing third-party risk to the financial authorities. Hence, the introduction of direct oversight frameworks for CSPs should not eliminate the obligations of financial firms under the indirect oversight approach. A balance needs to be achieved between having both direct and indirect approaches on the one hand and making sure that these do not lead to undue burden on CSPs (eg duplicative assurance processes) on the other hand. Table 2 summarises some key considerations for a direct oversight framework for critical CSPs.

[35] FSB (2023) proposes some criteria and tools for identifying systemic third-party dependencies and managing potential systemic risks from these dependencies.

Some key considerations for a direct oversight framework for critical CSPs to the financial sector

Table 2

Foundation	National ICT-related and/or cyber security requirements that apply across different sectors or cyber security requirements for financial firms.		
Relevant national authorities	National ICT authority – enforces technical requirements and standards for all ICT-related firms.	National cyber security authority – enforces the national cyber security requirements; brings specialised cyber security expertise.	Financial authorities – coordinate with national ICT and cyber security authorities in the development and enforcement of relevant requirements for critical CSPs. Should their legal mandates permit, financial authorities could consider introducing specific requirements on top of the requirements that apply across sectors to take into account financial system-specific concerns. For instance, such requirements could take into account the criticality of CSPs to the financial system (eg higher resilience standards, more frequent and intensive resilience testing, and incident response and recovery exercises).
Cross-border arrangements for the oversight of a critical CSP	May be necessary where (i) the CSP is considered critical in multiple jurisdictions where it operates and (ii) there are no restrictions on the CSP's use of data centres outside of a jurisdiction to service domestic customers. These cross-border arrangements can either be informal or formal.		
	Informal arrangements • Timely sharing of incidents or threats capable of having a systemic impact, where feasible subject to legal constraints. • Sharing of best practices such as resilient cloud adoption by the financial sector. • Development of cloud capability such as the understanding of cloud services, infrastructure and architecture. • Conduct of ad hoc cross-border resilience testing and incident response and recovery exercises. Could facilitate and coordinate cross-border response and recovery in the event of an actual incident.	Formal arrangements • Arrangement and agreement on timely sharing of incidents and threats. • Alignment and/or strengthening of resilience standards or requirements. • Conduct of required cross-border resilience testing and incident response and recovery exercises. Can deploy more preventative and corrective measures. Could facilitate and coordinate cross-border response and recovery in the event of an actual incident. Involvement of national ICT or cyber security authorities would be necessary if a jurisdiction's financial authorities do not have legal mandates for CSP oversight.	

Source: FSI analysis.

37. **National ICT or cyber-related requirements, where they are in place, can serve as an important foundation when establishing a direct oversight framework for critical CSPs given that**

CSPs' operations typically span across various sectors within a jurisdiction.[36] For example, as discussed above, some jurisdictions may have technical, financial and other requirements imposed on ICT-related services, including CSPs. Moreover, some jurisdictions may have cyber security requirements arising from national cyber security legislation that apply to different types of institutions, including CSPs. These requirements could serve as a basis or foundation for addressing the resilience issues posed by critical CSPs not just in the financial system but also across the economy.

38. **Authorities responsible for developing and implementing national ICT and cyber-related requirements have a role to play in the direct oversight of critical CSPs.**

- **The national authority in charge of a jurisdiction's ICT infrastructure may be naturally suited and better positioned to provide direct oversight of CSPs given the cross-sector operations of CSPs within the country/jurisdiction.** The national ICT authority possesses the right competencies to oversee CSPs and hence can facilitate alignment of technical requirements and standards, including resilience requirements, across all ICT-related services used or offered in the economy.
- **The national cyber security authority also plays an essential role in helping the national ICT authority develop and implement cyber security standards and best practices for CSPs to ensure that they are operating at the highest level of security and resilience.** For instance, the national cyber security authority can establish and enforce cyber-related regulations on CSPs and also facilitate cyber incident response and coordination, particularly for incidents with cross-sectoral impact, such as those involving critical CSPs.

39. **Financial authorities (ie a central bank or supervisory authority) can play a role in exercising the oversight of critical CSPs.** They can coordinate with national ICT or cyber security authorities in the development and enforcement of relevant requirements for critical CSPs.[37] Where their legal mandates permit, financial authorities can build on existing ICT and cyber-related requirements themselves by introducing additional requirements to take into account the criticality of CSPs to the financial system. Such additional requirements may include, for example, higher risk management or resilience standards or more frequent and intensive resilience testing and incident response and recovery exercises. Moreover, financial authorities may also adjust Annex F of the PFMI to tailor it to critical CSPs to the financial sector, similar to what is envisioned in the UK proposal.

40. **In engaging or overseeing CSPs, financial authorities need to recognise the important role of financial firms.** It is important that oversight does not end up being a dialogue just between financial authorities and CSPs. Financial firms should also be in the picture as the ultimate users of CSP services. There has to be regular interaction among all parties in order to have common understanding of financial authorities' concerns and expectations, how these are addressed by CSPs and how financial firms manage the risks posed to them.

41. **It is important that the relevant authorities in a jurisdiction work closely to ensure a consistent and holistic approach to the oversight of CSPs.** This is especially the case where a jurisdiction has no relevant horizontal authority (eg ICT or cyber security authorities) but rather relies on separate sectoral authorities. In either case, the presence of multiple national authorities overseeing CSPs may result in regulatory misalignment, presenting significant challenges for various stakeholders, including supervisory authorities and CSPs. For example, conducting effective oversight becomes more complex when multiple regulatory bodies are involved. CSPs also need to comply with multiple and potentially conflicting regulations, which can be resource-intensive and time-consuming. More importantly, when a critical CSP experiences an operational disruption, the presence of multiple relevant authorities should not

[36] See FSB (2023).

[37] This should not result in financial authorities becoming a pseudo enforcement arm of other areas of government, which would be legally problematic in many jurisdictions.

result in uncoordinated responses. It is important to have a pre-agreed collective response and recovery playbook, which involves CSPs and financial firms, so that flow of information is unimpeded and regulatory responses are coordinated. In addition, for jurisdictions with national critical infrastructure regulations or laws in place, sectoral authorities – including financial authorities – need to be mindful that their interventions are consistent and do not conflict with the overall national approach.

42. **Cross-border arrangements are necessary in the oversight of a critical CSP.** At the very least, regulatory expectations for CSPs, particularly those operating globally, should be aligned across jurisdictions whether these are directly or indirectly imposed. Moreover, cross-border arrangements are particularly necessary where (i) the CSP is considered critical in the jurisdictions where it operates and (ii) there are no restrictions on the CSP's use of data centres outside of a jurisdiction to service domestic customers. If such conditions exist, an operational disruption of a CSP may affect multiple jurisdictions, especially if they are serviced by the same CSP region. Global standard-setting bodies could play a role in identifying CSPs that may pose cross-border systemic concerns. Cross-border arrangements will ensure that there will be proper coordination mechanisms in place should such a disruption occur. Such arrangements will also help ensure that CSPs are subject to consistent regulations and standards across jurisdictions. Moreover, this will also avoid unnecessary duplication of work in dealing with CSPs, such as audits of CSPs requested by regulators. CSA (2023), for example, finds that 50% of financial firms have had to coordinate more than five regulatory audit requests with their CSPs, while 15% have had to deal with more than 15 requests.

43. **In broad terms, these cross-border arrangements can take two forms:**

- **Informal multilateral platform** – This could involve a loose grouping of financial authorities, either at the global or regional level, who meet regularly to discuss risks posed by specific CSPs to their respective and collective financial systems. The group's meetings could also be a venue for sharing best practices in reviewing CSP-related issues around ICT risk management and incident response and recovery. To foster collaboration and develop a two-way information-sharing protocol, representatives from the CSPs could also be included in the group. This would allow for a better understanding of the CSPs' security measures and enable the group to provide feedback and recommendations for improvement. Moreover, the group could also conduct ad hoc resilience testing and incident response and recovery exercises involving CSPs. The Financial Sector Cloud Resilience Forum for financial authorities in Asia established by MAS is an example of this informal multilateral platform.[38]
- **Formal multilateral oversight arrangements** – This could take the form of a collective oversight body for a specific CSP at the cross-border level. The oversight body may be comprised of financial authorities from jurisdictions where the CSP is considered critical and that allow such CSP to use data centres outside of their respective jurisdictions. The body could be tasked with aligning and/or strengthening resilience standards or requirements for the CSP (similar to Annex F of the PFMI), including for incident reporting. It could also conduct required cross-border resilience testing and incident response and recovery exercises involving the CSP. The organisation of this oversight body could be inspired by the regime put in place for the Society of Worldwide Interbank Financial Telecommunication (SWIFT) and CLS.[39] A supervisory college model could also be used to supervise and share information about critical CSPs.[40] Needless to say, this type of arrangements requires participating financial authorities to have legal mandates

[38] See MAS (2023).

[39] SWIFT is subject to oversight by central banks of the G10 countries, with the National Bank of Belgium as the lead overseer. CLS is regulated and supervised by the Board of Governors of the Federal Reserve System and the Federal Reserve Bank of New York, with an Oversight Committee comprised of 22 central banks.

[40] See BCBS (2018).

for CSP oversight. If this is not the case, involvement of national ICT or cyber security authorities would be necessary.

44. **Both types of cross-border arrangements can, in theory, do similar things.** The only difference is that a formal oversight arrangement could establish more binding requirements (eg on sharing incident reporting standards, resilience standards, testing etc). Formal arrangements may therefore be more useful in deploying more preventative and corrective measures. However, such arrangements could also pose more practical challenges given their more formal nature.[41] Nevertheless, either approach should be able to facilitate and coordinate cross-border incident response and recovery measures. As at the national level, it is important to have a pre-agreed collective response and recovery playbook at the international level in the event of an operational disruption of a CSP with cross-border systemic impact.

45. **Cross-border oversight arrangements can start at the regional level, allowing for a more targeted and manageable approach that can be scaled up as needed.** Such arrangements could, for example, be established for each CSP region or group of CSP regions that service multiple jurisdictions. However, multiple cross-border arrangements should not result in different requirements for a critical CSP. There is therefore a need to coordinate the establishment of such requirements at the global level. In addition, oversight activities targeted to a critical CSP should be coordinated across different cross-border arrangements.

Section 6 – Conclusion

46. **The inherent nature of public cloud environments, with their shared infrastructure and cloud customers' reliance on CSPs to manage and maintain the underlying infrastructure and services, brings forth unique challenges for customers including financial firms.** These risks include threats to data security and privacy, system availability, continuity of operations, interoperability, auditability and compliance with legal requirements. Given the unique characteristics of public cloud services, the risks that arise from public cloud usage need to be managed differently from traditional on-premises IT infrastructure risks. In addition, the continued growth in cloud adoption by financial firms and dependency on only a few major CSPs could pose a systemic risk to the financial sector.

47. **The prevalent indirect approach to the oversight of CSPs by financial authorities may not be sufficient to address the systemic risk originating from a concentration in the provision of cloud services by a few CSPs.** Notwithstanding that financial firms have a responsibility to ensure the availability, resiliency and security of their workloads in the public cloud under the shared responsibility model, CSPs also need to take steps to make the overall environment available and secure. Financial firms might not have full visibility into the risk management and control measures adopted by CSPs. In addition, while financial firms have measures at their disposal to ensure the availability and resilience of their cloud workloads, such as the adoption of a multi-zone and multi-cloud approach, such measures can lead to increased cost, complexity and resource demands to design and operate in different cloud environments. As such, financial firms alone do not have the ability to fully mitigate the impact of such concentration. Hence regulatory interventions may be needed.

48. **For risks that are not within the control of financial firms, particularly systemic risks, there is scope to consider a direct regulatory oversight framework for critical CSPs.** It is important for financial authorities to have an assurance or the means to ensure that financial stability risks due to a potential outage at a CSP are mitigated and addressed. A direct oversight framework can also help address inherent limitations in the indirect oversight approach, such as limitations of financial firms' assessment of CSP risks due to either market power or a huge gap in technical skills. However, to address the risk of

[41] See FSB (2023) for discussion of some challenges to cross-border supervisory cooperation.

moral hazard, the introduction of a direct oversight framework should not eliminate the obligations of financial firms under the indirect oversight approach. At the same time, care must be taken that this dual approach does not lead to inefficient assurance processes resulting in undue burden on CSPs.

49. **Ideally, this regulatory oversight framework should be cross-sectoral in nature given the cross-sectoral use of CSP services.** The use of CSPs is not limited to the financial sector; other sectors in the economy also engage the services of CSPs. It is noteworthy that some jurisdictions have already established authorities or regulatory frameworks that are directly applicable to CSPs. To avoid duplication of efforts, any introduction of direct oversight frameworks for CSPs should take these existing arrangements into consideration. At the same time, where their legal mandates permit, financial authorities may build on these cross-sectoral regulations to take into account financial sector-specific concerns.

50. **Cross-border cooperation arrangements in the oversight of critical CSPs are necessary.** A critical CSP may serve customers across multiple jurisdictions and, in doing so, may use data centres located in different jurisdictions. In such a case, the impact of an operational disruption of the CSP will not be limited to just one jurisdiction. Cross-border cooperation arrangements are therefore important. Such arrangements could be informal or formal. A more formal arrangement allows for more binding preventative and corrective measures such as resilience requirements and cross-border resilience testing. Both types of arrangements, however, could facilitate cross-border incident response and recovery measures. As a first step, global standard-setting bodies could play a role in identifying CSPs that may pose cross-border systemic concerns.

51. **In summary, the unique characteristics of public cloud services pose risks to financial firms, including threats to data security and privacy, system availability and continuity of operations.** While financial firms have a responsibility to ensure the availability and resilience of their cloud workloads, regulatory interventions may be needed to address some of the systemic risks arising from the use of cloud services in the financial sector. This could include a direct regulatory oversight framework for critical CSPs that builds on cross-sectoral regulations, with additional sector-specific requirements where necessary and feasible, and includes cross-border cooperation arrangements.

References

Bank of England and Financial Conduct Authority (BoE/FCA) (2021): *Operational resilience: impact tolerances for important business services*, March.

——— (2022): *Operational resilience: critical third parties to the UK financial sector*, 21 July.

Bank of Japan (BOJ) (2021): *Key considerations for risk management in using cloud services*, 8 March.

Basel Committee on Banking Supervision (BCBS) (2018): *Cyber-resilience: range of practices*, December.

——— (2021): *Principles for operational resilience*, March.

Cloud Security Alliance (CSA) (2023): *State of financial services in cloud*, 5 June.

Communications, Space and Technology Commission (CST) (2023): *Cloud computing services provisioning regulations*, October.

Crisanto, J, C Donaldson, D Garcia Ocampo and J Prenio (2018): "Regulating and supervising the clouds: emerging prudential approaches for insurance companies", *FSI Insights on policy implementation*, no 13, December.

Cyber Security Agency of Singapore (2022): "Review of the Cybersecurity Act and update to the Cybersecurity Code of Practice for CIIs", 4 March.

Dgtl Infra (2023): "Cloud regions and availability zones: explained", 12 October.

European Union (EU) (2022): "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011", 14 December.

Financial Stability Board (FSB) (2019): *Third-party dependencies in cloud services: considerations on financial stability implications*, 9 December.

——— (2020): *Regulatory and supervisory issues relating to outsourcing and third-party relationships*, 9 November.

——— (2023): *Enhancing third-party risk management and oversight: a toolkit for financial institutions and financial authorities – consultative document*, 22 June.

Gartner (2022): "Gartner says more than half of enterprise IT spending in key market segments will shift to the cloud by 2025", 9 February.

Google (2021): "Google Cloud study: cloud adoption increasing in financial services, but regulatory hurdles remain", 12 August.

Malaysian Communications and Multimedia Commission (MCMC) (2017): *Licensing guidebook*, 31 August.

——— (2021): *Information paper on regulating cloud services*, 17 December.

Ministry of Communications and Information (MCI) (2023): "Speech by Minister Josephine Teo at the MCI Committee of Supply Debate 2023", 28 February.

Monetary Authority of Singapore (MAS) (2021): "Advisory on addressing the technology and cyber security risks associated with public cloud adoption", 1 June.

——— (2023): "MAS establishes Financial Sector Cloud Resilience Forum", 5 April.

Office of the Government Chief Information Officer (OGCIO) (2021): *Practice guide for cloud computing security [ISPG-SM04]*, June.

Prenio, J and F Restoy (2022): "Safeguarding operational resilience: the macroprudential perspective", *FSI Briefs*, no 17, 25 August.

Stone Forest Business Advisors (2023): "Lessons learnt from Microsoft's Azure outage", 14 March.

Synergy Research Group (2023): "Q1 cloud spending grows by over $10 billion from 2022; the Big Three account for 65% of the total", 27 April.

US Department of the Treasury (2023): "The financial services sector's adoption of cloud services", 8 February.

Vietnam Business Law (2023): "Comments on draft Law on Telecom in Vietnam", 21 April.

Annex – List of jurisdictions hosting regions of at least one of the top three CSPs

Australia	France	Malaysia	South Africa
Bahrain	Germany	Mexico	South Korea
Belgium	Hong Kong SAR	Netherlands	Spain
Brazil	India	New Zealand	Sweden
Canada	Indonesia	Norway	Switzerland
Chile	Ireland	Poland	Thailand
China	Israel	Qatar	United Arab Emirates
Chinese Taipei	Italy	Saudi Arabia	United Kingdom
Finland	Japan	Singapore	United States