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.