New considerations for governing cloud services for financial institutions

Background and context

The emerging wave of global regulatory focus on cloud technologies appears to be making its way to the United States, after receiving increased regulatory attention in Asia and Europe. On August 23 2019, two US House Representatives formally called on the Financial Stability Oversight Council (FSOC) to consider drafting new regulations for direct oversight of cloud services providers (CSPs) for major banks and financial institutions. House members proposed amending the Dodd-Frank designation for systemically important financial market utilities (SIFMUs) to include CSPs, which would likely result in enhanced monitoring and reporting of the potential systemic risk these firms pose to the US financial system. This proposal demonstrates a shifting mindset in how lawmakers in the US are considering cloud regulation, moving from indirect coverage, such as state-level data requirements on sub-components of cloud, to more extensive and direct coverage at a federal level.

Public focus on components of cloud and information security has increased dramatically over the past years, and increasingly there appears to be calls for enhanced oversight of CSPs and technology vendors, and potentially the creation of a standalone agency to oversee activity. Highly publicized security incidents have driven consumers and regulators to demand increased accountability for CSPs. Data leaks, along with the increased commoditization of public and private data, have heightened awareness of the need to secure data.

CSPs are thus at a turning point in which they may be required to reevaluate how their services are managed. Moving forward, CSPs may be required to develop leading practices around recovery and resolution planning (RRP), resiliency, and cyber security for the cloud services provided to financial services clients. This additional regulatory burden may raise the barrier for a new entrant in the CSP space leading to an even heavier concentration of CSPs, already dominated by a few leading providers.

While the roll-out of potential regulation is to be determined, the House’s proposal marks a change in focus. This paradigm shift in cloud service regulation has the potential to impact CSPs and the financial institutions that they serve.
**What’s at stake?**

The increased demand for cloud services oversight is expected to impact the priorities and considerations for regulatory agencies, CSPs, financial services firms, and their customers. For financial services firms, RRP requirements have primarily centered on the ability to demonstrate all the capabilities outlined by the FRB in their SR-14 guidance\(^5\) and through supplementary guidance.\(^6\) While formulating their approach to the FRB’s guidance, certain elements of the capabilities will clearly be less significant for the CSPs (such as capital and liquidity requirements) given the nature of their business. However, other elements will require a sharper focus, including considerations related to:

- **Shared and outsourced services:**
  - How reliant are the CSPs on third-party vendors in order to provide their service?
  - In case of an occurrence of an “Event”, are critical assets, such as systems and services, identified clearly in order to provide a minimal viable service to customers?
  - What kind of business continuity plans and disaster recovery are in place?

- **Governance**
  - Is there a clear reporting structure with staff named and triggers defined if an “event” occurs?
  - Is there governance in place around third-party risk management?

- **Legal entity rationalization and separability**
  - Are CSPs reliant on intra-company services from non-domiciled legal entities to provide services to US/global clients?
  - Are intra-company relationships well defined and operations understood if a business unit needs to be sold?

- **Information systems**
  - Are procedures in place for data security and categorization based on the type of data being hosted on behalf of customers?
  - Are fail-safe mitigation strategies in place to secure and provide access to this data in the case of an “event”?

The considerations laid out in the initial FRB capability requirements should form part of a CSP’s operational risk decision making process in service continuity and resilience. In the wake of enhanced regulation, these questions should be revisited by each of the regulators, the CSPs, and their financial services customers.

*The widespread adoption of cloud computing has changed the way firms utilize and deploy technology. Widespread coverage on data leakages and cyber events is compelling the industry to re-focus priorities*
For regulatory agencies:

The current approach of relying on the CSPs to informally self-regulate has been challenging. In many cases, the CSPs are still attempting to comprehensively understand these new and unfamiliar requirements. Therefore, more prescriptive guidance may be required to achieve the desired results. For lawmakers, drafting an enforceable regulatory regime, which would address a CSP’s unique structure, the initial step maybe in recognizing the systemically important role that CSPs play in the broader US economy.

Regulatory agencies may want to consider how to implement RRP requirements for CSPs, given the systemic and critical role they play within financial services and the wider economy. Regulatory focus will likely shift toward operational capabilities of CSPs, resiliency, and governance practices that support their service models. As mentioned earlier, the regulators should strike a fine balance between holding the CSPs accountable to manage the risk and being mindful of creating further systemic risk by raising regulatory barriers to entry, which would in turn further exacerbate the concentration risk among the top CSPs. Regulatory agencies should consider ensuring that the CSP’s role in providing modern ‘Innovation environments’ for business experimentation is not inhibited by overly burdensome compliance obligations.

The transparency that may be demanded by the regulatory agencies could be transformational for the CSPs, particularly in the technology industry which is often centered on competitive advantage by protecting their intellectual property.

For cloud service providers:

Many global regulators are increasing turning their attention to CSPs, and so with increased regulatory oversight, CSPs should reconsider their broader product strategies and the role of risk and compliance support functions. Previously, CSP product development and sales have been primarily driven by increased demand in computing power, storage, innovation and cost reduction. With increased regulatory focus for both CSPs and their clients, CSPs may want to consider providing their end users “out-of-the-box” regulatory guidance on how to demonstrate that the way they use and employ the CSP products are compliant with the applicable regulations. CSPs that can effectively adhere to this level of regulatory scrutiny, including launching products with a clear demonstration of how the product complies with regulations across jurisdictions and financial services sectors, may ultimately be the ones who become the most compelling in the marketplace.

For banks and bank customers:

Many major financial institutions are increasingly considering public cloud adoption, and some have already grown reliant on cloud computing services for their data and operational needs. A disruption or failure that impacts a major CSP could pose systemic risk to the US financial system due to the lack of alternative providers and structural challenges that prevent the migration of data between service providers. Regulators may require banks to incorporate CSPs into their RRP activities by developing playbooks that describe plans in the event of a CSP failure scenario. Indeed, to date most institutions have treated the CSPs similarly to other third-party technology partners, including associated mitigants for vendor risk. However, given the critical role that the CSPs play in hosting large amounts of sensitive banking and customer information, and often hosting critical processes, institutions should continue to reassess how they are gaining sufficient oversight. With stronger CSP controls and governance, banks can be positioned to mitigate operational losses in the case of a disruptive cloud event. Additionally, this should be a major consideration for the banks as they consider adopting a multi-cloud strategy to balance the risk between multiple CSP vendors.

A SIFMU lens on Cloud Service Providers:

The FRB is tasked with monitoring and regulating market participants that present a systemic risk to the US financial system. The FSOC, of which the Chair of the FRB is a voting member, currently has the authority to designate SIFMUs as systemically important. Therefore, if the FSOC designates CSPs as SIFMUs to better understand the risks these companies pose to the financial services industry—which is well within their purview—the CSPs would then be required to provide more information and transparency to the regulators.
However, it is important to note there are major differences in how CSPs and SIFMUs provide services to the industry and the risks each provider poses. SIFMUs participate in transactions among banks, presenting potential capital, liquidity, and operational risks to their customers. CSPs present unique operational, reputational, and security risks if a data breach were to occur.

Although CSPs may at the outset, may not fall within the capital and liquidity focus areas of SIFMU oversight, the FSOC is required to review other operational considerations that may be applicable to CSPs, including:

The failure of or a disruption to the functioning of the CSPs now or in the future could create, or increase, the risk of significant liquidity or credit problems spreading into the financial markets.

If a CSP is deemed systemically important, the SIFMUs and the large banks that rely on that CSP may be required to submit information to the FRB on a regular basis so that the agency can monitor the potential systemic risk that CSP may pose to the financial system.

Based on these criteria, CSPs could be given similar regulatory treatment as SIFMUs. The outcome of the assessment may result in increased scrutiny for financial institutions use of cloud services.

**Next steps & considerations**

With the regulatory spotlight turning toward cloud resiliency and security, the race is on for CSPs and banks to define a governance framework that provides sufficient oversight and transparency. Depending on the implementation and roll-out approach, new regulations may become disruptive to operational and risk management practices for CSPs.

Financial institutions can consider taking the following steps to address cloud services risks:

- Perform an **assessment of your firm’s governance model of all cloud services leveraged**
- Develop **CSP related updates for your RRP playbook**
- Consider **external review of operational risks and controls** of cloud services to your financial institution
- Consider **alternate approaches** in the adoption of emerging technologies to facilitate adherence to regulatory compliance, such as deploying a multi-cloud strategy, Container based deployments etc.
- Develop a meaningful partnership between the CSPs and your Third-Party providers to develop **operational responsibilities’ matrices**, identifying security and operational risks and assigning transparent ownership and oversight of mitigating control activities
- Consider opportunities for **periodic testing of critical controls** in your processes that are operated by CSPs
The changing regulatory landscape for the financial services customers of cloud service providers will require careful reflection, meaningful action and deliberate preparation for the future

Endnotes
