PUBLICATION

Banking in the Cloud: How Financial Institutions Can Mitigate the Regulatory and Security Risks

Authors: Matthew George White
March 14, 2023

As organizations in the financial sector continue to migrate IT and business services to the cloud and adopt other cloud offerings, it is important that financial institutions understand the risks associated with each. A U.S. Treasury report issued on February 8, 2023, showed that regulators are closely monitoring how the financial sector uses cloud services. With cloud service providers becoming more assertive in shifting risks to their customers, financial institutions may experience higher levels of regulatory scrutiny.

Background

Over the past decade, the financial services sector has steadily migrated many information technology (IT) functions to cloud service providers — everything from video teleconferencing to internal communications to customer-facing applications. However, models of adoptions — and associated risk — vary widely across the sector. As the Financial Services Sector Risk Management Agency , the U.S. Department of the Treasury issued a report on February 8, 2023, assessing these risks and associated challenges affecting the financial sector.

At its most basic level, cloud computing is a means by which organizations can access on-demand network services and infrastructure without having to host their own servers. It is flexible and scalable, so companies can easily add or remove resources as needed. The financial sector, in particular, has found cloud services to be valuable for a range of purposes, such as supporting remote work and using cloud-native capabilities.

Financial institutions are motivated to increase cloud adoption due to benefits such as cost reduction, quicker deployment of new IT assets, faster product and service development, and improved security and resilience. However, these benefits bring with them both risks and other challenges that organizations in the financial sector should consider as they migrate their IT and business functions to the cloud.

Cloud Adoption in the Financial Sector

In its report, Treasury found — as a symptom of rapid adoption of cloud services across the sector — the vast majority of financial institutions have implemented cloud services, but at significantly varied maturity levels. A survey by the American Bankers Association (ABA) in 2021 revealed that more than 90 percent of banks surveyed reported maintaining some form of data, applications, or operations in the cloud. Furthermore, more than 80 percent of those surveyed reported being in the early stages of adopting cloud services. Only 5 percent of the surveyed banks described their use of cloud technology as mature.

Various types of cloud offerings — public, private, and hybrid — exist to cater to diverse service requirements. Public cloud, for instance, allows multiple customers, or "tenants," to share resources. Private cloud, by contrast, is an environment operated exclusively for a single organization, either on or off premises, and allows the cloud to be tailored to meet specific needs, such as security, compliance, or performance. A hybrid model incorporates both public and private cloud services alongside in-house data centers and is the preferred choice for many large financial institutions.

In contrast, some smaller and mid-sized institutions have adopted models using purely public cloud environments, significantly reducing their cost and data center usage but also increasing their risk. If set up properly, public cloud services can offer a resilient and secure setting. However, the level of resilience and security for a specific cloud service may differ dramatically depending on the provider, service, configuration, provisioning, and management. And, importantly, not all of these functionalities may be accessible in every situation.

Treasury's Findings

Treasury has highlighted six primary obstacles to the adoption of cloud technology in the financial industry:

1. Lack of transparency from cloud service providers, which makes it difficult for financial institutions to perform necessary due diligence, monitoring, and third-party risk management.
2. Shortage of human resources and tools to deploy cloud services securely, including issues such as user errors, a lack of skilled staff, and highly complex and non-user-friendly offerings.
3. Risk of operational incidents, which could arise from cross-geography incidents, such as identity and access management, or vulnerabilities in the cloud service offering.
4. Concentration of cloud service offerings with only a small number of providers, increasing the potential for aggregate impacts across the entire sector.
5. Weakened position for financial institutions when contracting with cloud service providers, given market concentration. Smaller to mid-sized institutions are particularly vulnerable to take-it-or-leave-it negotiations for cloud offerings.
6. Regulatory fragmentation at the international level posing risk to the security, resilience, and capabilities of cloud offerings used by U.S. financial institutions.

Treasury plans to take a number of steps to assist financial institutions in mitigation risk from the operational disruption of cloud services. As a preliminary step, Treasury plans to establish a Cloud Services Steering Group to address issues raised in this report. The Steering Group's functions will include:

- Promoting closer cooperation among U.S. regulators on cloud services.
- Conducting tabletop exercises with industry players.
- Reviewing incident protocols in light of growing reliance on cloud services.
- Measuring cloud service dependencies in the sector.
- Assessing systemic concentration and related risks on a sector-wide basis.
- Identifying ways to promote effective risk management practices in the financial services industry.

Action Steps

In light of this regulatory focus on how financial institutions are using cloud technologies, financial institutions can take several steps to mitigate the regulatory and security risks associated with cloud adoption.

- *Negotiate All Cloud Service Provider Contracts*: Often these agreements are presented as take-it-or-leave-it proposals. However, financial institutions should press to negotiate these agreements to ensure appropriate provisions are in place to mitigate risk. These provisions can include terms addressing security/privacy incident response and reporting, insurance requirements, audit rights, confidentiality, back-ups, audit rights, and assistance in regulatory inquiries. As regulators increase their focus in this area, financial institutions should use that fact to negotiate with cloud providers.
- *Diversify Use of Cloud Technologies*: Implementing a cloud solution can be an expensive and time-consuming process. However, in this context, the old adage "two is one, one is none" rings true. Deploying multiple cloud environments and spreading a financial institution's applications and data among those environments reduces the potential for a single point of failure in the event of a service outage or security incident.

- *Implement Robust Security Controls Addressing Cloud Environments*: While moving data to the cloud can increase an organization's overall security posture, financial institutions should not assume that this alone secures its data. Financial institutions should review their information security programs to ensure that specific protections such as access controls (including MFA), encryption, back-ups, and monitoring are in place, monitored, and enforced. Pairing robust internal security controls with known and monitored controls of a cloud service provider can be an effective way to secure sensitive data.
- *Regularly Assess Cloud Provider Compliance*: As noted above, audit rights should be negotiated in any cloud provider agreement. It is critical for financial institutions to not only negotiate to have these rights, but actually implement a regular process to ensure cloud providers are meeting requirements. Such a process can include requests for information, review of security policies and procedures, and conducting penetration testing. The specific tools a financial institution deploys to audit cloud service providers, and the timing of doing so, may differ from provider to provider based on the sensitivity of the information in the environment.
- *Train, Test, Repeat*: Employees should be trained on appropriate usage of cloud storage environments. Many times, the solutions offer a variety of tools for accessing data stored in the cloud. Employees should be instructed about when and what tools are permitted to be used and which are not (security controls should also prevent employee use of any tools that are not permitted). In addition, cloud environments should also be regularly tested to ensure they are securely storing applications and data. Another critical aspect of testing is to include the cloud environment in security incident tabletop testing. The results of these tests should be evaluated and used to improve a financial institution's overall security posture. Both employee training and testing should be repeated on a regular basis.

For any questions about how to manage security and risk in a cloud environment and how it might affect your business or your clients, or how you can prepare for these types of threats, please contact Matthew G. White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP or any member of the Baker Donelson Data Protection, Privacy, and Cybersecurity Team.