KPMG

Cloud service adoption for the financial service sector

Key takeaways from the Treasury department's report

July 2023

kpmg.com

Background

In February 2023, the US Department of the Treasury released a report on the financial services sector's adoption of cloud services. KPMG LLP has summarized the key messages and takeaways from this 71-page report. The report shares Treasury's findings on the current state of cloud adoption in the sector, including potential benefits and challenges associated with increased adoption. While this report does not impose new regulatory requirements or standards, it does reiterate the Regulators' stance that financial institutions (FIs) implement and manage risks to ensure operational resiliency as they undertake large-scale transformative programs such as cloud adoption. The report starts off with an executive summary in section 1, which includes the Treasury's Strategic Vision for Supporting the Resiliency of the Financial Sector's Use of Cloud Services.

After providing some background in section 2, the report discusses the use of cloud in financial services in section 3, specifically the motivation to use cloud and potential benefits of cloud.
In section 4, the report discusses the US domestic and international financial regulatory framework and in section 5 it highlights the typical practices followed by FIs when adopting cloud. In section 6, the report highlights the challenges with the financial sector's use of cloud services and, lastly, the planned next steps are noted in section 7.

Regulatory guidance is subject to change or modification, retroactively or prospectively, by varying interpretation and by subsequently issued pronouncements, legislation, and regulatory, administrative, or judicial decisions. We cannot guarantee that the regulatory authorities would agree with our analysis of this report.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS002209-1A

Key takeaways

FIs have discretion to leverage cloud service providers (CSPs); however, they also have responsibility for effective and appropriate management of technology operations and related risks, such as cybersecurity. The regulatory requirements place responsibility for effective and appropriate management of technology operations and related risks, such as cybersecurity, on FIs, regardless of whether any activities or operations are outsourced to third parties.

U.S. regulators' rules, regulations, and guidance applicable to cybersecurity and third-party risk management of FIs can take different forms depending on the issuing agency's statutory authority. For example, the SEC's Regulation Systems Compliance and Integrity (SCI) requires SCI entities to maintain business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse, and that are reasonably designed to achieve next-business-day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption. The regulatory requirements mentioned in section 4 are not new, but the takeaway here is how FIs are enforcing these requirements to manage risk when migrating and/or operating in the cloud. These risks can span the domains of security risk, vendor risks, resiliency risks, privacy risks, etc. Our point of view is that while risk domains remain the same, the specific guardrails and controls that FIs will need to apply in the cloud will differ significantly from on-premises technologies. A strong governance framework is a critical part of a FI's cloud journey. This governance framework will manage and control the use of cloud through enhanced policies, processes, and standards for operating within the cloud.

In Section 5, the report describes typical processes that FIs follow when adopting cloud services. Specifically, it includes practices adopted by FIs in the following three categories:

- **Risk management and operational resilience:** FIs should enhance their risk management processes across their first and second lines of defense. These may include conducting risk-based due diligence on the CSP and its services, establishing cloud governance processes, enhancing internal and external security and resiliency controls, and enforcing monitoring over the use cloud services. Additionally, a thorough third-party risk management program is necessary to deal with the cloud providers, specifically the smaller software-as-a-service providers.
- **Deployment and configuration:** FIs must ensure their use of public cloud is leveraging the CSP-provided options to gain higher operational resilience, for example, auto-scaling capabilities. FIs should set up the appropriate guardrails and security controls to restrict access and protect the data. FIs should also seek to reduce their long-term reliance on a specific CSP by architecting their applications and data for portability to other CSPs.
- **Monitoring, auditing, and testing:** FIs should implement appropriate monitoring capabilities in the cloud for continuous observability into their state of security, controls, and compliance. Regular periodic audits and technical assessments should be coupled with dashboard-level view into compliance and security posture for public cloud assets for application owners to effectively manage regulatory requirements.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS002209-1A

The report highlights the following six key challenges with FIs' use of cloud:

1. **Insufficient transparency to support due diligence and monitoring:** FIs are demanding additional information from CSPs to improve their understanding of risks associated with cloud services. These include risks related to CSPs' internal software dependencies, subcontractor and supply chain risks, CSP protection against pervasive vulnerabilities, etc. CSPs may never fully disclose the inner operations of their environment, and hence customers need to carefully review and be knowledgeable about their contracts with CSPs and the risks that they may have to deal with.
2. **Gaps in human capital and tools to securely deploy cloud services:** The Treasury notes the lack of cloud technical talent and lack of portability of cloud skills across CSPs and, therefore, inability of cloud customers to own their portion of the "Shared Responsibility Model". This has resulted in cloud misconfigurations by the cloud customers and, therefore, security incidents. KPMG recognizes this challenge across industries and suggests adequate involvement of system integrators and cybersecurity consultants to augment existing in-house skills to manage the skills gap.
3. **Exposure to potential operational incidents:** One of the critical risks pointed out by the Treasury is pervasive large-scale operational incidents at CSPs that affect multiple geographic regions or global CSP services such as identity and access management. KPMG recommends that FIs, at a minimum, be ready for scenarios involving temporary regional loss of cloud provider services. This includes multizone, and where necessary multiregion, high-resiliency architectures. Help ensure adequate backups, and draft and rehearse incident response/recovery processes. For extended multiregion failures, FIs should consider architecting their cloud workloads to enable portability to other CSPs or on-premises technologies.
4. **Potential impact of market concentration:** The current cloud services market is highly concentrated into a few CSPs and that exacerbates the risk of operational incidents as noted above. Treasury also believes there are opportunities to enhance public-private coordination given the broader trends in cloud adoption. For example, many organizations have not yet incorporated CSPs into sectorwide protocols for incident response
5. **Dynamics in contract negotiation given market concentration:** Treasury states that FIs have expressed challenges in the negotiation of contracts with CSPs. This includes inability to negotiate right to audit clause, avoid termination by CSP without adequate notice, etc. The Treasury will continue to assess this issue, as it believes that unbalanced contractual terms could limit customers' ability to measure and mitigate risk from cloud services.
6. **International landscape and regulatory fragmentation:** International regulatory concern over cloud services has the potential to prevent globally active US FIs from deploying cloud services across their overall enterprise, including their foreign operations.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS002209-1A

Next steps

As a part of its future considerations, the Treasury highlights a few steps it will take in future that include the following:

Establishing an interagency Cloud Services Steering Group

Facilitating further engagement between financial sectors and CSPs

Driving closer cooperation between US regulators on cloud services

Organizing tabletop exercises involving CSPs and the financial sector

Reviewing sectorwide incident protocols, including developing approaches for incident response involving cloud services to expand communication between US regulators, CSPs, and FIs

Considering ways to appropriately measure cloud services dependencies

Assessing systemic concentration and related risks

Developing relevant standards and international policies

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS002209-1A

How KPMG can help financial institutions achieve a secure and compliant cloud journey

It is clear from the Treasury's report that the regulators will be organizing themselves as an interagency Cloud Services Steering Group to provide a deeper level of oversight for FIs that adopt cloud. In the interim, the regulators will continue their respective supervision and examinations of FIs' technology and cyber risk management programs.

KPMG has helped FIs meet their cybersecurity, controls, and risk management responsibilities. We bring years of experience in helping clients manage the challenges and risks indicated by Treasury. KPMG is helping several FIs realize cloud benefits with a three-phased approach towards security, controls, and compliance:

- Developing cloud security, risk management, resilience, and governance capabilities
- Supporting cloud deployments and configuration related to security, resiliency, and privacy
- Assisting with ongoing cloud security operations as well as incident response.

Our capabilities in this space range from cloud security architecture and engineering to controls design for all the cloud service layers. Additionally, KPMG has alliance relationships with a range of leading cloud security technology vendors. In addition to the core CSPs, this includes technologies such as Cloud Security Posture Management, Security Orchestration and Automated Response, and Detection and Response. By marrying our risk management practices with leading technology implementation capability, KPMG is able to help our clients manage and mitigate their cyber risk in the cloud.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS002209-1A

Contact us

Sai Gadia
Partner, Advisory
Cyber Security Services,
KPMG LLP
E: sgadia@kpmg.com

Steve Barlock
Principal, Advisory
Cyber Security Services,
KPMG LLP
E: sbarlock@kpmg.com

Niranjan Girme
Director, Advisory
Cyber Security Services,
KPMG LLP
E: ngirme@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS002209-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

KPMG LLP does not provide legal services.