Regulatory Alert

Regulatory Insights

September 2021

Regulatory focus on cloud computing

Key points

Regulatory agencies are taking note of the speed and scale with which financial services companies are transitioning to cloud computing – as well as the predominance of a few, very large cloud service providers – and have begun to highlight certain key areas of concern for maintaining safe and sound operations, data security, and consumer data protections. Consistent themes across the agencies address ***cybersecurity, data privacy, third-party management, and business continuity****. Key considerations include companies' ultimate responsibility for compliance with all applicable laws and regulations; the selection, oversight, testing, and review of third-party service providers; the clarity and thoroughness of both company and cloud provider responsibilities documented in contracts; data security through authentication and access controls; and plans for potential service interruptions/data breaches and mitigation of concentration risk. Companies should ensure they have a defined data strategy and inventory for cloud computing, and that their cloud program is integrated with the business objectives across all divisions and processes.*

Recent regulatory releases and actions include:

- **FINRA study | Cloud computing in the securities industry.** The Financial Industry Regulatory Authority (FINRA) published the results of a study designed to shed light on the state of cloud adoption within the securities industry and related implications. The study included "nearly 40 market participants operating in this space, including broker-dealer firms, cloud service providers, industry analysts, and technology consultants." The report highlights:
  - **Common themes** related to cloud adoptions:
    - "Off-the-shelf" cloud products are commonly used for non-core business functions
    - Rollouts of cloud infrastructure tend to be targeted, incremental, and iterative
    - Enhanced cloud-focused governance and policies and procedures are developed to safeguard data and systems in the cloud environment
    - Reassessment of technology expertise, including staff training and recruiting needs, often coincide with cloud adoption.
  - **Regulatory considerations** related to cloud adoption and migration:
    - **Cybersecurity** – cybersecurity should be incorporated as a critical component of the evaluation, development, and testing process of any cloud-based application and the division of tasks (e.g., threat detection, incident response, patching/updating) should be reflected in the contractual agreement between the firm and cloud services provider
    - **Data privacy** – policies and procedures related to customer data privacy, including those related to vendor agreements, may need to be

updated based on changes to how customer data is collected, stored, analyzed, and shared

- **Outsourcing/vendor management** – outsourcing an activity or function to a cloud service provider or other cloud vendor does not relieve a firm of its ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA rules associated with the outsourced activity or function. Firms should be cognizant of concentration risk and consider multi-cloud or hybrid cloud options as appropriate, as well as exit strategies to mitigate against an unfavorable lock-in scenario
- **Business continuity** – written business continuity plans relating to an emergency or significant business interruption are required to be reviewed and updated annually. The cloud is thought to offer the potential for greater business resiliency due to redundant storage and computing capacity across cloud service provider's data centers though firms should consider testing the redundant configuration to ensure business services can continue in the face of a disruption, and update test plans and procedures accordingly
- **Recordkeeping** – recordkeeping obligations (e.g., retention periods, format, media) should be considered when assessing recordkeeping products or services offered by a cloud provider.

— **Request for comment** by October 16, 2021, including identification of any matters the commenter believes it would be appropriate for FINRA to consider guidance, "consistent with the principles of investor protection and market integrity," related to cloud computing applications and their implications for FINRA rules.

— **FFIEC guidance | Authentication and Access to Financial Institution Services and Systems.** The members of the Federal Financial Institutions Examination Council (FFIEC) issued updated guidance on effective **authentication and access** risk management principles and practices. The guidance responds to significant risks associated with the expanded cybersecurity threat landscape, which are attributed in part to the use of application programming interfaces (APIs) and increasing connectivity to third parties such as cloud service providers. It is directed toward all users with access to digital banking systems and financial institution information systems, including business and retail customers, employees, third parties, and system-to-system communications. (*See KPMG Regulatory Alert, available here*)

— **Proposed interagency guidance | Third-Party Relationships: Risk Management**. The FRB, FDIC, and OCC jointly issued proposed guidance on managing risks associated with **third-party relationships**, including relationships with financial technology-focused entities. The proposed guidance describes third-party relationships as business arrangements between a banking organization and another entity, by contract or otherwise. Frequently Asked Questions (FAQs) that may be incorporated into the guidance clarify that cloud service providers are third parties, a firm's **due diligence and oversight** should be commensurate with the risk of the activity or data using the cloud computing, and that **responsibilities should be clearly documented** in the contract. Further, due diligence and oversight should be conducted to confirm that the third-party cloud service provider can satisfactorily oversee and monitor any cloud service subcontractor. (*See KPMG Regulatory Alert, available here*)

- The agencies have separately released guidance specifically directed to community banks on **Conducting Due Diligence on Financial Technology Companies**.

— **FFIEC Statement | Security in a Cloud Computing Environment.** The members issued this joint statement to address the use of cloud computing services and security risk management principles in the financial services sector. It highlights the importance of sound security controls and management's understanding of the shared responsibilities between cloud service providers and their financial institution clients. Examples of risk management practices and controls, including safeguards to protect customers' sensitive information from risks that pose potential consumer harm, are provided covering a variety of areas, including:

- **Governance** – The financial institution's plans for the use of cloud computing services should align with its overall IT strategy, architecture, and risk appetite. Institutions should not expose themselves to more risk than defined by their risk appetite without appropriate risk mitigation measures.
- **Cloud security management** – There are often key security considerations and controls that are unique to cloud computing environments; examples are provided across due diligence, oversight and monitoring, contractual

responsibilities, inventory process, identity and access management, sensitive data controls, and training.

- **Change management**, systems migration – Cloud implementation often uses microservices, which may pose security, reliability, and latency issues; having multiple microservices can increase the financial institution's attack surface. Management should evaluate implementation options that meet the institution's security requirements.
- **Resilience and recovery**, incident response – Resiliency and recovery capabilities are not necessarily included in cloud service offerings; therefore, the contract should outline the resiliency and recovery capabilities required by the institution. Based on the cloud service contract, management should evaluate and determine how cloud-based operations impact both the business continuity plan and recovery testing plans; these plans should be updated and subject to regular tests and validation. Cloud service contracts should similarly specify activities for incident response and each party's responsibilities.
- **Audit and controls** assessment (regular testing for critical systems, monitoring of cloud service provider controls, interoperability and portability, data destruction and sanitization).

— **Financial Technology Summit on Cloud Computing**. The Federal Reserve Bank of Richmond has scheduled a Financial Technology Summit on Cloud Computing for September 29 and 30 of this year. The event will feature panel discussions on topics including cloud adoption, **cybersecurity** and data in the cloud**, business resiliency** and **third-party risk management** in the pandemic and post-pandemic environment, and innovation and collaboration in the cloud.

— **COSO ERM Framework | Enterprise Risk Management for Cloud Computing.** COSO, the Committee of Sponsoring Organizations of the Treadway Commission, issued guidance on *Enterprise Risk Management for Cloud Computing*, which is intended to serve as a guide to establishing cloud computing governance by leveraging the principles of COSO's *Enterprise Risk Management – Integrating with Strategy and Performance* framework (as updated in 2017).

COSO suggests the use of the COSO ERM framework enables cloud computing to be integrated with the organization's ERM function. The guidance explains how to apply cloud computing governance across each of five components in the COSO ERM framework (i.e., 1) governance and culture, 2) strategy and objective setting, 3) performance, 4) review and revision, and 5) information, communication, and reporting.) A "roadmap" to implement cloud computing (Appendix A. Roadmap to Cloud Computing) and descriptions of roles and responsibilities are included as appendices. (Appendix B. Roles and Responsibilities).

For additional information please contact Amy Matsuo or Sailesh Gadia.

Amy Matsuo
Principal and Leader
ESG and Regulatory Insights
E: amatsuo@kpmg.com

Contributing authors:
Amy Matsuo, Principal and Leader, ESG and Regulatory Insights

Karen Staines, Director, Regulatory Insights

kpmg.com/socialmedia