PUBLICATION

Critical Guidance for Financial Institutions on Security Considerations for Cloud Computing Environments

Authors: Matthew George White
May 01, 2020

On April 30, 2010, the Federal Financial Institutions Council (FFIEC) issued Guidance on the use of cloud computing services and security risk management principles in the financial services sector. The Guidance reminds member institutions of the importance of effective risk management for the safe and effective use of cloud computing services and should be viewed as a "call to action" in the continued review of information security controls.

Over the last several years, financial institutions have increasingly moved towards utilizing cloud-based networks and services. Without proper protections in place, these services can create risks and make sensitive customer information vulnerable. Given the increased use of remote access and cloud-based services as a result of COVID-19 concerns, these risks are only increased. We previously provided steps for financial institutions to take to mitigate these risks in alerts available here, here, and here, and additional information is available on Baker Donelson's Coronavirus (COVID-19): What You Need to Know information page of our website.

The FFIEC Guidance highlights examples of risk management practices for a financial institution's safe and sound use of cloud computing services and safeguards to protect customers' sensitive information from risks that pose potential consumer harm. In addition, the FFEIC Guidance reminds financial institutions (and their subcontractors and vendors) of the importance of due diligence in selecting cloud-based service providers. Among the key areas of importance are:

1. The contractual agreement(s) which should define service expectations and the vision of control responsibilities of both parties; and

2. Ongoing oversight and monitoring of the relationship, including auditing/testing and evaluation of corrective actions.

Examples of risk management practices provided in the Guidance include:

- Align cloud computing services with the institution's overall IT strategy. This includes determining the division of governance responsibilities, which systems and information should be considered for cloud computing services, and how these services will be monitored. Institutions should also keep an inventory to track the systems and information residing in the cloud.

- Ensure appropriate due diligence is conducted before selecting a cloud-based service provider, and engage in ongoing monitoring and oversight during the term of the relationship. Critical in this process are controls for testing and auditing the security controls of the provider. Where direct testing is not possible or permitted, consider using independent audit providers.

- Include contractual provisions that clearly delineate the responsibilities of each party. Provisions should address (among other things): access rights, configuration capabilities, responsibility for

encryption keys, security monitoring, system testing/updating, auditing, and incident response.

- Engage in regular testing and monitoring of the cloud environment's controls. Misconfiguration of cloud resources is a prevalent vulnerability and can result in placing sensitive customer information at risk. Institutions should ensure the systems they are utilizing are properly configured and are regularly tested to ensure a secure cloud computing environment.

- Implement controls to ensure appropriate data access. There are a variety of controls that institutions should consider implementing to limit access to data stored on the cloud. These include designating different levels of access for different account types, multi-factor authentication, encryption, and data tokenization. In a cloud environment, encryption of sensitive data is extremely important, as is ensuring appropriate management of encryption keys.

Other important risk management practices addressed in the Guidance include employing security awareness and training programs to educate staff, implementing controls for the transition of systems and information to the cloud, ensuring the systems have appropriate resiliency and recovery capabilities, and developing and testing incident response plans that account for cloud-specific challenges, such as technology assets owned or managed by third-party service providers.

Finally, the Guidance delineates additional risk management controls unique to cloud computing environments. These controls include:

- Implementing appropriate controls over virtual infrastructure;

- Deploying specific security measures to address vulnerabilities present when using containers;

- Using managed security services, such as cloud access security broker (CASB) tools;

- Considering the interoperability and portability of data and services and how to appropriately scale security measures to address these capabilities; and

- Applying appropriate procedures (and ensuring cloud vendors do the same) for the destruction and sanitation the institution's data.

While cloud-based services can provide extraordinary convenience for financial institutions, it is critical that these services are only deployed after appropriate safeguards and controls are put in place. If you have any questions about how to implement or protect a cloud-based system, or other concerns about data protection or cybersecurity, please contact Matthew G. White, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.