Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • www.ffiec.gov

Joint Statement

FFIEC Joint Statement on Risk Management for Cloud Computing Services

INTRODUCTION

The Federal Financial Institutions Examination Council (FFIEC) on behalf of its members[1] is issuing this statement to address the use of cloud computing[2] services and security risk management principles in the financial services sector. Financial institution management should engage in effective risk management for the safe and sound use of cloud computing services. Security breaches involving cloud computing services highlight the importance of sound security controls and management's understanding of the shared responsibilities between cloud service providers and their financial institution clients.

This statement does not contain new regulatory expectations; rather, this statement 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. Management should refer to the appropriate FFIEC member guidance referenced in the "Additional Resources" section of this statement for information regarding supervisory perspectives on effective information technology (IT) risk management practices. This statement also contains references to other resources, including the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Department of Homeland Security (DHS), International Organization for Standardization (ISO), Center for Internet Security (CIS), and other industry organizations (e.g., Cloud Security Alliance).

BACKGROUND

Due diligence and sound risk management practices over cloud service provider relationships help management verify that effective security, operations, and resiliency controls are in place and consistent with the financial institution's internal standards. Management should not assume that effective security and resilience controls exist simply because the technology systems are operating in a cloud computing

[1] The FFIEC comprises the principals of: the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

[2] NIST SP 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction.

environment. The contractual agreement between the financial institution and the cloud service provider should define the service level expectations and control responsibilities for both the financial institution and provider. Management may determine that there is a need for controls in addition to those a cloud service provider contractually offers to maintain security consistent with the financial institution's standards.

Ongoing oversight and monitoring of a financial institution's cloud service providers are important to gain assurance that cloud computing services are being managed consistent with contractual requirements, and in a safe and sound manner. This oversight and monitoring can include evaluating independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments), and evaluating corrective actions to confirm that any adverse findings are appropriately addressed. Risk management expectations for the management of relationships involving third parties (such as third-party cloud computing services) are outlined in FFIEC members' respective guidance and the Information Security Standards.[3]

Cloud computing environments are enabled by virtualization[4] technologies, which allow cloud service providers to segregate and isolate multiple clients on a common set of physical or virtual hardware. Financial institutions use private cloud computing environments,[5] public cloud computing environments,[6] or a hybrid of the two. NIST generally defines three cloud service models.[7] For each service model, there are typically differing shared responsibilities between the financial institution and the cloud service provider for implementing and managing controls. These models and the typical responsibilities include:

- **Software as a Service (SaaS)** is similar to traditional outsourcing in which the software applications (applications) operate on the provider's cloud infrastructure. In this model, financial institution management does not typically manage, maintain, or control the underlying cloud infrastructure or individual application capabilities. The financial institution is responsible for user-specific application configuration settings, user access and identity management, and risk management of the relationship with the cloud service provider. The cloud service provider is responsible for any changes to and maintenance of the applications and infrastructure.

- **Platform as a Service (PaaS)** is a model in which a financial institution deploys internally developed or acquired applications using programming languages, libraries, services, and tools supported by the cloud service provider. These applications reside on the provider's platforms

[3] A financial institution's overall information security program must also address the specific information security requirements applicable to "customer information" set forth in the "Interagency Guidelines Establishing Information Security Standards" implementing section 501(b) of the Gramm–Leach–Bliley Act and section 216 of the Fair and Accurate Credit Transactions Act of 2003. See 12 CFR 30, appendix B (OCC); 12 CFR part 208, appendix D-2, and 12 CFR part 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA) (collectively referenced in this statement as the "Information Security Standards").
[4] The NIST Glossary defines virtualization as the simulation of the software and/or hardware upon which other software runs.
[5] The NIST Glossary defines private cloud computing as "The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."
[6] The NIST Glossary defines public cloud computing as "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."
[7] NIST SP 800-145, The NIST Definition of Cloud Computing.

and cloud infrastructure. PaaS models necessitate similar risk management as the SaaS model. However, management is also responsible for appropriate provisioning and configuration of cloud platform resources and implementing and managing controls over the development, deployment, and administration of applications residing on the provider's cloud platforms. The cloud service provider is responsible for the underlying infrastructure and platforms (including network, servers, operating systems, or storage).

- **Infrastructure as a Service (IaaS)** is a model in which a financial institution deploys and operates system software, including operating systems, and applications on the provider's cloud infrastructure. Like PaaS, the financial institution is responsible for the appropriate provisioning and configuration of cloud platform resources and implementing and managing controls over operations, applications, operating systems, data, and data storage. Management may need to design the financial institution's systems to work with the cloud service provider's resilience and recovery process. Also, as in the other models, the financial institution is responsible for risk management of the relationship with the cloud service provider. The cloud service provider is responsible for controls related to managing the physical data center. For example, the cloud service provider updates and maintains the hardware, network infrastructure, environmental controls (e.g., heating, cooling, and fire and flood protection), power, physical security, and data communications connections. Additionally, cloud service providers are typically responsible for managing the hypervisor(s).[8]

These examples describe typical shared responsibilities for the different service models; however, the specific services and responsibilities will be unique to each service deployment and implementation. Regardless of the environment or service model used, the financial institution retains overall responsibility for the safety and soundness of cloud services and the protection of sensitive customer information.[9]

RISKS

In cloud computing environments, financial institutions may outsource the management of different controls over information assets and operations to the cloud service provider. Careful review of the contract between the financial institution and the cloud service provider along with an understanding of the potential risks is important in management's understanding of the financial institution's responsibilities for implementing appropriate controls. Management's failure to understand the division of responsibilities for assessing and implementing appropriate controls over operations may result in increased risk of operational failures or security breaches. Processes should be in place to identify, measure, monitor, and control the risks associated with cloud computing. Failure to implement an effective risk management process for cloud computing commensurate with the level of risk and complexity of the financial institution's operations residing in a cloud computing environment may be an unsafe or unsound practice and result in potential consumer harm by placing customer-sensitive information at risk.

[8] NIST defines a hypervisor as the virtualization component that manages the guest operating systems (OSs) on a host and controls the flow of instructions between the guest OSs and the physical hardware. A function of the hypervisor is to logically separate virtual machines from each other in the virtual network.

[9] *See* the Information Security Standards:12 CFR 30, appendix B (OCC); 12 CFR part 208, appendix D-2, and 12 CFR part 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA).

RISK MANAGEMENT

Examples of relevant risk management practices for assessing risks related to and implementing controls for cloud computing services include:

Governance

- **Strategies for using cloud computing services as part of the financial institution's IT strategic plan and architecture.** The financial institution's plans for the use of cloud computing services should align with its overall IT strategy, architecture, and risk appetite. This includes determining the appropriate level of governance, the types of systems and information assets considered for cloud computing environments, the impact on the financial institution's architecture and operations model, and management's comfort with its dependence on and its ability to monitor the cloud service provider.

Cloud Security Management

- **Appropriate due diligence and ongoing oversight and monitoring of cloud service providers' security.** As with all other third-party relationships, security-related risks should be identified during planning, due diligence, and the selection of the cloud service provider. Management should implement appropriate risk management and control processes to mitigate identified risks once an agreement is in place. The process for risk identification and controls effectiveness may include testing or auditing, if possible, of security controls with the cloud service provider; however, some cloud service providers may seek to limit a financial institution's ability to perform their own security assessment due to potential performance impacts. Management can leverage independent audit results from available reports (e.g., system and organizational control[10] (SOC) reports). Additionally, management can use the security tools and configuration management capabilities provided as part of the cloud services to monitor security. While risks associated with cloud computing environments are typically similar to traditional outsourcing arrangements, there are often key security considerations and controls that are unique to cloud computing environments.

- **Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider.** Contracts between the financial institution and cloud service provider should be drafted to clearly define which party has responsibilities for configuration and management of system access rights, configuration capabilities, and deployment of services and information assets to a cloud computing environment, among other things. When defining responsibilities, management should consider management of encryption keys, security monitoring, vulnerability scanning, system updates, patch management, independent audit requirements, as well as monitoring and oversight of these activities and define responsibility for these activities in the contract. Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data

[10] Developed by the AICPA, system and organization controls (SOC) reviews refer to the audits of system-level controls of a third-party service provider.

at contract termination, and restrictions on the geographic locations where the financial institution's data may reside.

- **Inventory process for systems and information assets residing in the cloud computing environment.** An effective inventory process for the use of cloud computing environments is an essential component for secure configuration management, vulnerability management, and monitoring of controls. Processes to select and approve systems and information assets that are placed in a cloud computing environment should be established to ensure that risks are appropriately considered. An inventory management process to track systems and information assets residing in the cloud computing environment, including virtual machines, application programming interfaces, firewalls, and network devices can allow management to better manage and safeguard information assets.

- **Security configuration, provisioning, logging, and monitoring.** Misconfiguration of cloud resources is a prevalent cloud vulnerability and can be exploited to access cloud data and services.[11] System vulnerabilities can arise due to the failure to properly configure security tools within cloud computing systems. Financial institutions can use their own tools, leverage those provided by cloud service providers, or use tools from industry organizations to securely configure systems, provision access, and log and monitor the financial institution's systems and information assets residing in the cloud computing environment. Cloud computing may involve different security control configurations and processes than those employed in more traditional network architectures. Regardless of the configurations, tools, and monitoring systems employed, a key consideration is the regular testing of the effectiveness of those controls to verify that they are operating as expected. Management can use available audit or assurance reports to validate that testing is performed. Management may consider leveraging cloud computing standards and frameworks from industry standard-setting organizations to assist in designing a secure cloud computing environment while considering risk.[12]

- **Identity and access management and network controls.** Common practices for identity and access management for resources using cloud computing infrastructures include limiting account privileges, implementing multifactor authentication, frequently updating and reviewing account access, monitoring activity, and requiring privileged users to have separate usernames and passwords for each segment of the cloud service provider's and financial institution's networks. Default access credentials should be changed, and management should be aware of the risk of overprovisioning access credentials. Access to cloud tools for provisioning and developing systems, which may contain sensitive or critical bank-owned data should be limited. Examples of network controls include virtual private networks, web application firewalls, and intrusion detection systems. Management should consider implementing tools designed to detect security misconfigurations for identity and access management and network controls.

- **Security controls for sensitive data.** Controls (e.g., encryption, data tokenization,[13] and other

[11] In the National Security Agency's "Mitigating Cloud Vulnerabilities," the report notes that misconfigurations of cloud resources include policy mistakes, a misunderstanding of responsibility and inappropriate security controls.
[12] For example, refer to NIST's Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014.
[13] Data tokenization refers to the practice of substituting sensitive data with a random value, or token that is associated with the sensitive data.

data loss prevention tools) to safeguard sensitive data limit a malicious actor's ability to exploit data during a breach. When using data encryption controls in a cloud computing environment, management should consider defining processes for encryption key management between the financial institution and the cloud service provider. Many cloud service providers offer cloud-based key management services, which allows integration with other cloud-based services. However, cloud-based key management services may allow administrators from a cloud service provider to access encrypted information. For this reason, management may elect to use the financial institution's own encryption and key management services. The trade-off is that non-cloud-based encryption should be built into the application to work properly and application-based encryption may impede automated controls offered by cloud service providers. Common methods to manage encryption in cloud computing environments include the use of hardware security modules,[14] virtual encryption tools, cloud-based security tools, or a combination of these.

- **Information security awareness and training programs.** Training promotes the ability of staff to effectively implement and monitor necessary controls in the cloud computing environment. A wide range of resources are generally available to management, including information and training obtained from external, independent organizations on the use of cloud technologies. Management may also consider using product-specific training provided by cloud service providers to educate staff on product-specific security tools.

Change Management

- **Change management and software development life cycle processes.** Change management controls are important for effectively transitioning systems and information assets to a cloud computing environment. Management may augment existing change management processes and the software development life cycle (SDLC), as applicable, for cloud computing environments.

- **Microservice[15] architecture.** Though not unique to cloud application development, cloud implementation often uses microservices to develop applications with smaller, lighter-weight code bases that facilitate faster, more agile application development. However, there are security, reliability, and latency issues with microservices, and having multiple microservices can increase the financial institution's attack surface.[16] Management should evaluate implementation options that meet the institution's security requirements.

Resilience and Recovery

- **Business resilience and recovery capabilities.** Operations moved to cloud computing environments should have resilience and recovery capabilities commensurate with the risk of the service or operation for the financial institution. Management should review and assess the resilience capabilities and service options available from the cloud service provider. There may

[14] A hardware security module is a physical computing device that implements security functions, including cryptographic algorithms and key generation.
[15] NIST Glossary defines a microservice as a set of containers that work together to compose an application.
[16] *NIST Special Publication 800-204 Security Strategies for Microservices-based Application Systems* provides additional technical details for financial institutions considering the use of microservices.

be several configurations available, and management should determine which options best meet the institution's resilience and recovery requirements. Resilience and recovery capabilities are not necessarily included in cloud service offerings; therefore, the contract should outline the resilience and recovery capabilities required by the institution. Based on the cloud service model used, management should evaluate and determine how cloud-based operations affect both the business continuity plan and recovery testing plans. As with other operations, management should regularly update business continuity plans to reflect changes to configurations and operations and regularly test and validate resilience and recovery capabilities. Testing may need to be conducted jointly with the provider depending on the service model being used.

- **Incident response capabilities.** The financial institution's incident response plan should take into account cloud-specific challenges due to ownership and governance of technology assets owned or managed by the cloud service provider. The contract should define responsibilities for incident reporting, communication, and forensics. Cloud usage presents unique forensic issues related to jurisdiction, multi-tenancy, and reliance on the cloud service provider for a variety of forensic activities. Additionally, the service level agreement should identify specific activities for incident response and identify the cloud service provider's responsibilities in the event of an incident. When responding to an incident, management should recognize shared responsibilities and corresponding duties. Often, cloud service providers offer a variety of monitoring and alerting tools that can be leveraged by a financial institution and integrated into its incident response plans.

Audit and Controls Assessment

- **Regular testing of financial institution controls for critical systems.** Processes should be in place for regular audit and testing of security controls and configurations commensurate with the risk of the operations supported by the cloud service. These processes can include the audit and testing of the financial institution's security configurations and settings, access management controls, and security monitoring programs.

- **Oversight and monitoring of cloud service provider-managed controls.** Management should evaluate and monitor the cloud service provider's technical, administrative, and physical security controls that support the financial institution's systems and information assets that reside in the cloud environment. Oversight and monitoring activities include requesting, receiving, and reviewing security and activity reports from the cloud service provider; reports of compliance with service level agreements; product validation reports; and reports of independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments) performed on the cloud computing services. Other considerations may include personnel controls (e.g., background checks and security awareness training) for staff that supports the financial institution's operations or has access to financial institution data. Management may test the cloud service provider's controls if permitted by the contract. Where there is a limited ability to directly monitor or test the security controls managed by the cloud service provider, management may obtain SOC reports, other independent audit reports, or ISO certification reports to gain assurance that the controls are implemented and operating effectively. Management should understand the scope of independent assurance testing to determine whether the scope is comprehensive and the reports contain sufficient information for management to evaluate the

cloud computing services.

- **Controls unique to cloud computing services.** While many of the controls outlined in this statement also apply to more traditional network architectures, there are controls unique to the architectures of cloud computing services. Examples of such controls include:

    - **Management of the virtual infrastructure.** The ability to create secure virtual infrastructures is managed through cloud security tools, such as the hypervisor, and should be closely controlled by the cloud service provider. The cloud service provider should be able to provide assurance that it has appropriate controls over the hypervisor, or other virtual infrastructure controls, to manage the cloud services being provided to the financial institution. For example, management should consider verifying whether cloud service providers scan their hypervisor code for vulnerabilities and monitor system logs. This can be accomplished by management or through reviews of available third-party assurance reports.
    - **Use of containers[17] in cloud computing environments.[18]** The advantages of using containers in a cloud-computing environment include portability and less memory utilization compared to using separate virtual machines (VMs). However, "[w]hile containers provide a strong degree of isolation, they do not offer as clear and concrete of a security boundary as a VM. Because containers share the same kernel and can be run with varying capabilities and privileges on a host, the degree of segmentation between them is far less than that provided to VMs by a hypervisor."[19] Therefore, when using containers, management should consider:
        - Storing data outside of the container, so that data do not have to be re-created when updating and replacing containers.
        - Verifying that configurations prevent containers from unintentionally interacting.
        - Securing containers from applications within them.
        - Securing the host from containers and vice versa.
        - Monitoring containers for vulnerabilities and updating or replacing containers when appropriate.

      Additionally, traditional security controls, such as firewalls and intrusion detection systems, may not be effective because containers may obscure activities; therefore, container-specific security solutions should be implemented.
    - **Use of managed security services for cloud computing environments.** Financial institutions may choose to leverage available security tools and services to assist with managing and monitoring security for cloud computing services. Common tools and services include use of cloud access security broker (CASB)[20] tools. For more information on managed security service providers, refer to "Outsourcing Technology

[17] NIST Glossary defines containers as a method for packaging and securely running an application within a virtualized environment. *NIST SP 800-190 Application Container Security Guide* states "The term is meant as an analogy to shipping containers, which provide a standardized way of grouping disparate contents together while isolating them from each other."
[18] *NIST Special Publication 800-190 Application Container Security Guide* provides additional technical details for financial institutions considering the use of containers.
[19] *NIST SP 800-190 Application Container Security Guide*.
[20] Cloud access security brokers are generally products or services that monitor activity between cloud service users and cloud applications and can typically be used to enforce security policies, alert for anomalous activity or monitor performance.

Services – Appendix D" of the *FFIEC IT Examination Handbook.*

- **Consideration of interoperability[21] and portability[22] of data and services.** When selecting or designing and building cloud computing services, management may consider interoperability and portability in the design of those services or application providers. A financial institution's interoperability and portability strategy will depend on the institution's risk appetite and the contracted service model (e.g., SaaS, PaaS, or IaaS) employed. Management may consider these capabilities as part of the initial contracting and design of cloud computing services.
- **Data destruction or sanitization.** Institutions should be aware of the processes that the cloud service provider uses for data destruction. The service level agreement should outline that adequate measures are taken to ensure data destruction is done in a manner that would prevent unauthorized disclosure of information.

ADDITIONAL RESOURCES

The risk management considerations outlined in this statement provide a summary of key controls that management may consider as part of assessing and implementing cloud computing services. However, specific risk management and controls will be dependent on the nature of the outsourced services and the specifics of the cloud implementation. Additional information on general third-party risk management and outsourcing practices is available in the *FFIEC Information Technology Examination Handbook's "*Outsourcing Technology Services" booklet and other documents published by FFIEC members.

There are also many industry-recognized standards and resources that can assist financial institutions with managing cloud computing services. Examples of these include NIST, the Center for Internet Security's Critical Security Controls, and the Cloud Security Alliance. Management may research and consider consulting industry-recognized standards and resources when developing and implementing security controls in a cloud computing environment.

[21] NIST 500-291, version 2: *NIST Cloud Computing Standards Roadmap* defines interoperability as the capability of data to be processed by different services on different cloud systems through common specifications.

[22] NIST 500-291, version 2: *NIST Cloud Computing Standards Roadmap* defined portability the ability for data to be moved from one cloud system to another or for applications to be ported and run on different cloud systems at an acceptable cost.

REFERENCES

U.S. Government Resources

FFIEC

FFIEC Information Technology Examination Handbook

FFIEC "Outsourced Cloud Computing" (July 10, 2012)

National Institute of Standards and Technology

NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing

NIST 800-145: The NIST Definition of Cloud Computing

NIST 800-146: Cloud Computing Synopsis and Recommendations

NIST 800-125: Guide to Security for Full Virtualization Technologies

NIST 800-125A Rev.1: Security Recommendations for Server-based Hypervisor Platforms

NIST Special Publication 800-125B: Secure Virtual Network Configuration for Virtual Machine (VM) Protection

NIST Special Publication 800-190: Application Container Security Guide

National Security Agency

Mitigating Cloud Vulnerabilities

Department of Homeland Security CISA

Microsoft Office 365 Office Security Observations

Cloud Security Guidance

The Basics of Cloud Computing

General Services Administration

Federal Risk and Authorization Management Program (FedRAMP)

Industry Resources

Center for Internet Security (CIS) Controls v.7 (Control 7)

Cloud Security Alliance

Institute of Electrical and Electronics Engineers (IEEE) Cloud Computing Standards

International Organization for Standardization (ISO)

OWASP