FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2018-04: CLOUD COMPUTING RISK MANAGEMENT

Purpose

This advisory bulletin provides Federal Housing Finance Agency (FHFA) guidance to Fannie Mae, Freddie Mac, the Federal Home Loan Banks (FHLBanks), and the Office of Finance (OF) (collectively, the regulated entities)[1] on assessing and managing risks associated with third-party cloud providers. Effective risk management of cloud providers is critical to safe and sound operations. Each regulated entity should use a risk-based approach across key areas listed below to meet FHFA supervisory expectations:

I. Governance
   A. Responsibilities of the Board and Senior Management
   B. Strategies, Policies, Procedures, and Internal Standards
II. Third-Party Cloud Provider Management
   A. Due Diligence Assessment
   B. Service Agreements
   C. Oversight and Ongoing Monitoring
III. Information Security
   A. Shared Responsibility for Security
   B. Data Classification and Systems Security
   C. Access Management
   D. Incident Notification, Planning, and Response
   E. Development and Testing Environments
IV. Business Continuity Cloud Provider Management

[1] The OF is not a "regulated entity" as the term is defined in the Federal Housing Enterprises Financial Safety and Soundness Act. *See* 12 U.S.C. 4502(20). However, for convenience, references to the "regulated entities" in this advisory bulletin should be read to apply also to the OF.

Background

Cloud computing is 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 service provider interaction. This model is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (Software as a Service or SaaS, Platform as a Service or PaaS, and Infrastructure as a Service or IaaS), and four deployment models (private cloud, community cloud, public cloud, and hybrid cloud).[2]

Relationships between cloud customers and their cloud providers are complex. Critical information and resource controls may shift from in-house operations to a third party, meaning the regulated entity and cloud provider share responsibility for safeguarding organizational information and systems. Additionally, cloud providers may have privileged access to organizational systems and information. Because of this shared responsibility, a regulated entity engaging with a cloud provider should take appropriate steps to manage associated third-party risks and revise the information security program to address risks specific to cloud computing. A regulated entity should also prepare for outages and failures that may hinder access to organizational information and systems that rely on cloud providers.

FHFA's general standards for safe and sound operations are set forth in the Prudential Management and Operations Standards (PMOS) at 12 CFR Part 1236 Appendix. Three relevant PMOS articulate guidelines for a regulated entity's board of directors and management to evaluate when establishing internal controls and information systems (Standard 1), overall risk management processes (Standard 8), and maintenance of adequate records (Standard 10).

Guidance

FHFA expects each regulated entity to appropriately manage its cloud computing risks as part of its enterprise-wide risk management program,[3] and in accordance with all relevant FHFA guidance. Application of this guidance by the regulated entity should correspond to the level of risk presented. The regulated entity's evaluation of the level of risk should include the classification of the data hosted at the cloud provider, the criticality of the service(s) provided,

[2] *See* Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145 for definitions of terms related to cloud computing.

[3] 12 CFR 1239.11(a)(risk management program) requires each regulated entity to establish a board-approved enterprise-wide risk management program under which an entity may establish particular practices, procedures, or programs to manage specific types of risk, such as cloud computing risks. The regulation does not set requirements for the particular practices, procedures, or programs established for managing particular risks under the enterprise-wide risk management program.

service and deployment models used, and other risks associated with engaging a third-party cloud provider.

The regulated entity may establish a standalone cloud computing risk management program or subsume the governance and functions of cloud computing risk management under another established program. The complexity of and level of risk associated with the regulated entity's cloud usage should inform the decision on whether the cloud computing risk management program should exist as a standalone program or is subsumed into other program(s). Because cloud computing affects several different areas of operations, those responsible for managing related risks should coordinate across different divisions to manage the third-party provider, information security, and business continuity risks.

I. Governance

The governance of the cloud computing risk management program should consist of the cloud strategy, policies, procedures, and internal standards. If the regulated entity subsumes the governance of the cloud computing risk management program into other programs, the regulated entity should clearly communicate which strategies, policies, procedures, and internal standards apply. The complexity of and level of risk associated with the regulated entity's cloud usage should inform whether the board or senior management approves the cloud computing strategy, policies, procedures, and internal standards.

A. Responsibilities of the Board and Senior Management

The board of directors or a committee thereof (board) should provide oversight to the cloud computing risk management program. As part of that oversight, the board should understand the risks involved in the regulated entity's use of cloud computing. The board should ensure that senior management fully understands the effects of shifting to a cloud computing environment and has appropriate expertise on managing those effects prior to engaging a cloud provider. The board should review the strategy or strategic plan that covers cloud computing and major policies relating to associated risks.

Senior management should develop and periodically update policies, procedures, and internal standards and implement the cloud computing risk management program. Senior management should also periodically report to the board about the nature of the regulated entity's cloud computing risk, which may change significantly over time.

B. Strategies, Policies, Procedures, and Internal Standards

Each regulated entity should establish and periodically update its cloud computing strategy, and evaluate its appetite for associated risks. The regulated entity's current and planned cloud usage,

including the extent and purpose, the classification of data stored on the cloud, and the choice of cloud service and delivery model, should inform the development of individual policies, procedures, and internal standards. Policies should describe appropriate uses for cloud computing. The regulated entity should evaluate and update policies, procedures, and internal standards so they are consistent with the cloud strategy and the regulated entity's risk appetite.

The regulated entity should develop or update internal standards as a basis for managing and monitoring risks at levels consistent with the regulated entity's risk appetite. The internal standards should establish the technical and operational criteria the regulated entity uses to evaluate cloud provider service agreements and controls, including criteria on performance and reliability in terms of availability, security, business continuity, and compliance. Where possible, internal standards should include metrics. The regulated entity should consider industry standards as well as its needs, capabilities, and risk appetite to inform the development of its internal standards.

II. Third-Party Cloud Provider Management

The regulated entities should take steps to mitigate the third-party risks arising from their use of cloud providers. The shared responsibility framework, heightened administrative privileges, standardized service model, and potential for vendor lock-in of cloud providers, result in new risks and complications to existing risks.

A. Due Diligence Assessment

In addition to an evaluation of financial, operational, legal, compliance, and reputational risks of engaging the cloud provider, the regulated entity should evaluate whether and how shifting to a cloud computing environment affects risk. If warranted under the circumstances, the assessment should include a comparison with other cloud providers that offer comparable services. The results of due diligence assessments should frame service agreement negotiations and the regulated entity's procedures and operations for managing provider-specific cloud computing risks.

The on-demand self-service and rapid elasticity of cloud service have the potential to result in substantial changes to the risks associated with a specific cloud provider when the service agreement has not changed. Consequently, due diligence assessments should occur for every cloud provider at contract inception and prior to any modifications in the level or type of services obtained that could result in significant increases to the regulated entity's risk exposure. Policies on the frequency of due diligence assessments should also consider the rapid evolution in the market for cloud services.

B. Service Agreements

Recognizing that each cloud computing use, complexity, and risk is unique, the details of the service agreement provisions may vary. Because cloud providers often use a standardized service model, the regulated entity may not be able to negotiate changes to the selected cloud provider's standard service agreement. In cases where there are differences between the chosen cloud provider's service agreement and the regulated entity's policies and internal standards, the regulated entity should first consider alternative providers. If a regulated entity determines that no alternatives exist that meet the business need, the regulated entity should develop plans to mitigate or transfer any risks emanating from the differences to reduce the risk to an acceptable level.

Service agreements with a cloud provider should define roles and responsibilities of the cloud provider and regulated entity. Service agreements should not restrict information technology, information security, and business continuity teams from effectively performing their responsibilities in the cloud environment, including monitoring and evaluating performance, protecting against and responding to security incidents, and supporting ongoing risk and compliance management.

Prior to executing a cloud computing service agreement, legal and information security experts who are knowledgeable about cloud computing should review the agreement to determine if the agreement exposes the regulated entity to unacceptable levels of risk. The review should include an assessment of significant contractual risk points for cloud computing, such as the dispute resolution process, confidentiality provisions, privacy policy, data residency, and any limitations on liability, indemnities, termination rights, and suspension rights. Additionally, the review should include a determination of whether and how the cloud provider may use regulated entity data for its own purposes. In accordance with a regulated entity's policies and procedures, the regulated entity should re-evaluate service agreements periodically to determine whether they need to be updated.

C. Oversight and Ongoing Monitoring

The regulated entity should implement and oversee ongoing monitoring to ensure compliance with the service agreement(s) and to evaluate the performance of the cloud provider. The regulated entity should track all cloud providers used, the approved cloud services, and usage of those services. Each entity should assess each cloud provider's quality and performance in providing information security to protect data at rest and in transit and evaluate the timeliness and completeness of the provider's communications.

If the regulated entity relies on monitoring and oversight provided by third parties, such as third party audit reports, the regulated entity should evaluate whether its contracted cloud services

match the services evaluated in the outsourced monitoring and oversight.

III. Information Security

Migrating operations to the cloud may result in both new information security risks, such as from multi-tenancy risks, and complications to existing information security risks, such as risks stemming from privileged user access. The regulated entity should evaluate and revise its information security program to reflect its cloud computing environments, and it should, to the extent possible, extend information security governance, engineering, architecture, and operations to cloud computing environments and providers.

A. Shared Responsibility for Security

The regulated entity and the cloud provider share responsibility for protecting data stored in the cloud. The regulated entity should understand its cloud security responsibilities, which may vary based on the provider and service model. In addition to any descriptions of the roles and responsibilities in the service agreement, the terms of the cloud provider's information security standards and controls should inform the regulated entity of its responsibilities for protecting its cloud environment(s). The regulated entity should understand and mitigate, accept, or transfer the risks from any identified gaps in the cloud provider's information security program.

B. Data Classification and Systems Security

The data classification and the regulated entity's risk appetite should inform the security requirements of specific data in the cloud. Prior to placing data in a cloud environment, the regulated entity should evaluate the appropriateness of its protections, such as encryption, and geographic location of data at rest and in transit. The regulated entity should assess compliance with its security policies through regular tests of key controls, systems, and procedures it uses for its cloud environment(s).

The regulated entity should comply with laws and other requirements that may restrict where data are stored and establish appropriate data storage controls designed to maintain data in the appropriate physical location. Additionally, there are substantial legal and security risks to storing data outside the United States. The regulated entity should evaluate its risk appetite, the applicable jurisdiction's laws, and the regulated entity's expertise in and ability to effectively mitigate the security and legal risks prior to permitting hosting data in a jurisdiction outside of the United States.

The service and deployment model may also inform decisions about security requirements. For example, some cloud environments share physical components and resources among disparate

tenants using logical separation of data. To protect against multi-tenancy risks, the regulated entity should ensure that it and the cloud provider take steps such as using information technology services and systems to monitor applicable activity within the cloud environment.

C. Access Management

Cloud computing environments may differ in access management configurations, so each regulated entity should take steps to ensure that identity and access management functions are configured properly. The regulated entity should evaluate the effectiveness of policies, procedures, and internal standards on identity and access management functions to protect against unauthorized or malicious use by the cloud provider.

The regulated entity should protect and secure cloud credentials. When encrypting data in the cloud, the regulated entity should protect and secure encryption keys in a manner consistent with the classification of the data they protect.

D. Incident Notification, Planning, and Response

The regulated entity should update its incident response plan(s) to include incidents that could arise from using cloud providers. Responding to incidents that occur in the cloud environment often requires coordination with the cloud provider. Notification requirements in the service agreement should define the criticality of the incidents the cloud provider should report and require the cloud provider to deliver timely notification of such incidents with sufficient detail to allow the regulated entity to take steps to prevent the expansion of an incident, mitigate its effects, or eradicate the incident in accordance with its incident response plan.

E. Development and Testing Environments

Regulated entities that isolate testing and development environments may maintain less rigorous controls over these environments to increase flexibility for developers and testers. The regulated entity should revisit and, as appropriate, update policies, procedures, and internal standards for development and testing on the cloud to assess whether it has sufficient controls to maintain security at all phases of the development life cycle.

IV. Business Continuity Cloud Provider Management

Cloud computing services may experience outages and performance slowdowns. The regulated entity should configure its cloud usage for a level of availability and reliability appropriate for its intended use. Using a cloud provider for disaster recovery does not relieve the regulated entity of its business continuity responsibilities. Business continuity scenarios and associated plans

should evaluate a variety of scenarios, including permanent cloud provider failure, as well as a range of short- to long-term disruptions. The regulated entity should test, using an appropriate testing method, its business continuity plan both prior to, and while relying on, the cloud provider(s) for operations.

Each regulated entity should consider the risk of using the same cloud provider for multiple critical services. If an FHLBank plans to rely on another FHLBank (*e.g.*, Buddy Bank) for business continuity and both use the same cloud provider, these arrangements should be re-evaluated for the possibility of a simultaneous disruption.

Related Guidance

Information Security Management, Federal Housing Finance Agency Advisory Bulletin 2017-02, September 28, 2017.

Internal Audit Governance and Function, Federal Housing Finance Agency Advisory Bulletin 2016-05, October 7, 2016.

Data Management and Usage, Federal Housing Finance Agency Advisory Bulletin 2016-04, September 29, 2016.

Information Technology Investment Management, Federal Housing Finance Agency Advisory Bulletin 2015-06, September 21, 2015.

Model Risk Management, Federal Housing Finance Agency Advisory Bulletin 2013-07, November 19, 2013.

Operational Risk Management, Federal Housing Finance Agency Advisory Bulletin 2014-02, February 18, 2014.

12 CFR Part 1236 Prudential Management and Operations Standards, Appendix.

12 CFR Part 1239.11(a)(risk management program).

FHFA has statutory responsibility to ensure the safe and sound operations of the regulated entities and the Office of Finance. Advisory bulletins describe FHFA supervisory expectations for safe and sound operations in particular areas and are used in FHFA examinations of the regulated entities and the Office of Finance. Questions about this advisory bulletin should be directed to: SupervisionPolicy@fhfa.gov.