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

NOTE: This document, issued by the FFIEC Information Technology Subcommittee, is for information purposes only. July 10, 2012

Outsourced Cloud Computing

Summary

The Federal Financial Institution Examination Council Agencies consider *cloud computing* to be another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing. This paper addresses the key risks of outsourced cloud computing identified in existing guidance.

Cloud computing is a relatively new term used to describe a variety of established business strategies, technologies, and processing methodologies. Although the term cloud computing is gaining in usage, there is no widely-accepted definition,[1] and numerous business strategies, technologies, and architectures are represented as cloud computing. In general, cloud computing is a migration from owned resources to shared resources in which client users receive information technology services, on demand, from third-party service providers via the Internet "cloud."

Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. These models include: a private cloud, which is operated solely for an organization; a community cloud, which is shared by several organizations; a public cloud, which is available to any paying customer; and a hybrid cloud, which is a composition of two or more clouds (private, community, or public).

Financial institutions that contemplate or use a cloud computing model in which all or part of the service is outsourced ("*outsourced cloud computing*") have to consider the fundamentals of risk and risk management defined in the *FFIEC Information Technology Examination Handbook* (IT Handbook), especially the Outsourcing Technology Services Booklet ("Outsourcing Booklet").

[1] In December 2011, the National Institute for Standards and Technology (NIST) issued Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing." In this publication, NIST defines cloud computing "as a model for enabling 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 cloud provider interaction."

The following discussion addresses the key elements of outsourced cloud computing implementation and risk management as they relate to the Outsourcing Booklet.

Due Diligence

A financial institution's use of third parties to achieve its strategic plan does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations.

Outsourcing to a cloud service provider can be advantageous to financial institutions because of potential benefits such as cost reduction, flexibility, scalability, improved load balancing, and speed. Before approving any outsourcing of significant functions, it is important to ensure such actions are consistent with the institution's strategic plans and corporate objectives approved by the board of directors and senior management.

As detailed in the Outsourcing Booklet, a due diligence review is performed to ensure that the provider will meet the institution's requirements in terms of cost, quality of service, compliance with regulatory requirements, and risk management. The following are potential issues related to cloud computing:

- **Data classification:** How sensitive is the data that will be placed in the cloud (e.g., confidential, critical, public) and what controls should be in place to ensure it is properly protected? Does the cloud service provider appropriately encrypt or otherwise protect non-public personal information (NPPI) and other data whose disclosure could harm the institution or its customers?
- **Data segregation:** Will the financial institution's data share resources with data from other cloud clients? For example, will the data be transmitted over the same networks, and stored or processed on servers that are also used by other clients? If so, what controls does the service provider have to ensure the integrity and confidentiality of the financial institution's data?
- **Recoverability:** How will the service provider respond to disasters and ensure continued service? Do the financial institution's disaster recovery and business continuity plans include appropriate consideration of this form of outsourcing, the service provider's disaster recovery and business continuity plans, and the availability of essential communications links?

Vendor Management

Managing a cloud computing service provider may require additional controls if the servicer is unfamiliar with the financial industry and the financial institution's legal and regulatory requirements for safeguarding customer information and other sensitive data. Additionally, the use of such a servicer may present risks that the institution is unable or unwilling to mitigate. One example of such risks would be if the servicer is not

implementing changes to meet regulatory requirements. Under such circumstances, management may determine that the institution cannot employ the servicer.

Disengagement of a service provider is another aspect of vendor management that can be complicated in cloud computing, particularly for smaller financial institutions. It is important that contracts and service level agreements are specific as to the ownership, location(s) and format(s) of data, and dispute resolution.

Audit

To effectively evaluate the risk and risk mitigation associated with the use of third-party servicers, a financial institution must determine the adequacy of a servicer's internal controls. Auditors assist in this evaluation by assessing whether those controls are functioning appropriately.

A financial institution's audit policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing. Also, it may be necessary to augment the internal audit staff with additional training and personnel with sufficient expertise in evaluating shared environments and virtualized technologies.

Information Security

As with other forms of outsourcing, information security implications are key considerations in the cloud computing model. Financial institutions may need to revise their information security policies, standards, and practices to incorporate the activities related to a cloud computing service provider. In high-risk situations, continuous monitoring may be necessary for financial institutions to have a sufficient level of assurance that the servicer is maintaining effective controls.

It is important that financial institutions maintain a comprehensive data inventory and a suitable data classification process, and that access to customer data is restricted appropriately through effective identity and access management. A multi-tenant cloud deployment, in which multiple clients share network resources, increases the need for data protection through encryption and additional assurance that proper controls are in place to restrict tenant access solely to their respective data. Verifying the data handling procedures, the adequacy and availability of backup data, and whether multiple service providers are sharing facilities are important considerations. If financial institutions are not sure that their data are satisfactorily protected and access to their data is appropriately controlled, entering into a third-party relationship with such servicer may be ill advised.

Storage of data in the cloud could increase the frequency and complexity of security incidents. Therefore, management processes of financial institutions should include effective monitoring of security-related threats, incidents, and events on both financial institutions' and servicers' networks; comprehensive incident response methodologies; and maintenance of appropriate forensic strategies for investigation and evidence collection.

The potential that data are not completely removed or deleted from the servicer's storage media at the conclusion of a service contract may pose higher risk in a cloud computing environment than it does in more traditional forms of outsourcing. Before entering into a third-party relationship, it is prudent to ensure that the cloud-computing service provider can remove NPPI from all locations where it is stored.

Legal, Regulatory, and Reputational Considerations

Important considerations for financial institutions before deploying a public cloud computing model include clearly identifying and mitigating legal, regulatory, and reputational risks. The nature of cloud computing may increase the complexity of compliance with applicable laws and regulations because customer data may be stored or processed overseas. A financial institution's ability to assess compliance may be more complex and difficult in an environment where the cloud computing service provider processes and stores data overseas or comingles the financial institution's data with data from other customers that operate under diverse legal and regulatory jurisdictions. A financial institution should understand the applicability of laws and regulations within the hosting countries and the financial institution's ability to control access to its data. Contracts with the cloud-computing service providers should specify the servicers' obligations with respect to the financial institutions' responsibilities for compliance with privacy laws, for responding to and reporting about security incidents, and for fulfilling regulatory requirements to notify customers and regulators of any breaches.

Business Continuity Planning

The business continuity planning process in a financial institution involves the recovery, resumption, and maintenance of the entire business, including outsourced activities. When considering outsourcing to a cloud-computing service provider, financial institutions need to determine whether the servicer and the network carriers have adequate plans and resources to ensure the financial institution's continuity of operations, as well as its ability to recover and resume operations if an unexpected disruption occurs.[2]

Conclusion

The fundamentals of risk and risk management defined in the IT Handbook apply to cloud computing as they do to other forms of outsourcing. Cloud computing may require more robust controls due to the nature of the service. When evaluating the feasibility of outsourcing to a cloud-computing service provider, it is important to look beyond potential benefits and to perform a thorough due diligence and risk assessment of elements specific to that service. Vendor management, information security, audits, legal and regulatory compliance, and business continuity planning are key elements of sound risk management and risk mitigation controls for cloud computing. As with other service provider offerings, cloud computing may not be appropriate for all financial institutions.

[2] For further information, refer to the "Business Continuity Planning" section in the Outsourcing Booklet.