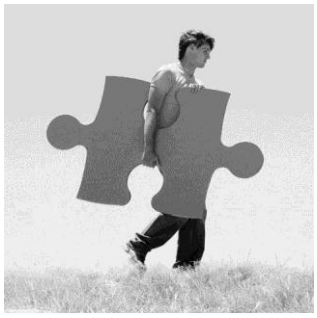
News Bulletin

July 10, 2012



Federal Financial Agencies Issue Cautionary Statement on Financial Institution Cloud Computing Services

On July 11, 2012, the federal financial regulatory agencies ("Agencies"),[1] through the Federal Financial Institutions Examination Council ("FFIEC"), issued a joint interagency statement ("Statement") on the use by financial institutions of outsourced cloud computing services, and the key risks associated with such services.[2] The Statement, the substance of which is also being incorporated into the FFIEC's Information Technology Examination Handbook ("IT Handbook"),[3] is the first formal federal financial agency statement on the matter of cloud computing, a subject that has garnered substantial attention in the financial services industry but that, to date, has not been formally addressed by the federal financial regulators. In general, the Statement reaffirms that the fundamentals of existing risk and risk management requirements that currently are applicable to financial institution outsourcing of IT services apply equally to outsourced cloud-based services, while identifying certain risks that, in the Agencies' view, are of particular concern with respect to such services.

Cloud Computing – An Overview

Cloud computing is an IT delivery model where IT services are provided to users from remote servers and facilities over the Internet rather than through owned or leased IT servers and platforms. The cloud technology offers important benefits to users, including the chance for significant cost savings and operational efficiencies; flexibility in deployment; ready access to information systems, applications, and data; better backup services; and faster and more responsive upgrade functionalities. Through cloud computing services, users have the ability to outsource all or part of their IT hardware architecture (infrastructure as a service, or IaaS), operating systems and platforms (platform as a service, or PaaS), or software applications (software as a service, or SaaS) as they choose. "Clouds" can be private, where the services are operated solely for one organization (or a small group of organizations, which some refer to as "community" clouds), typically on a dedicated or partitioned platform; public, where the services are shared by numerous customers, and typically operated on a shared platform; or hybrid, which entails a combination of private and public cloud services.

Potential hosts such as major IT service providers see very significant business opportunities in cloud computing, and as a result, the interest in, and demand for, cloud computing services has increased dramatically over the past

[1] Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and the State Liaison Committee.
[2] FFIEC, Information Technology Subcommittee, Statement on Outsourced Cloud Computing (July 10, 2012).
[3] *See*, IT Handbook, *Outsourcing Technology Services*, Appendix A, "Examination Procedures" and Appendix D, "Managed Security Service Providers."

several years.[4] At the same time, financial institutions have increasingly recognized the potential technological, legal and regulatory challenges, including information security, data integrity and privacy, and business continuity issues, associated with their use of remote IT services for core operations and storage of critical and sensitive data. In turn, these challenges have caused financial institutions, especially those in the United States, to move cautiously toward cloud-based solutions.

The Statement

Up until now, specific financial regulatory guidance on financial institutions' use of cloud-based IT services has been almost nonexistent. As a result, financial institutions have effectively had to "interpolate" general regulatory guidance on IT outsourcing[5] in their evaluation and use of cloud-based IT services. Therefore, the Agencies' Statement is a useful start in filling in the regulatory gaps on this topic, although the Statement's guidance is relatively short on specifics and may not tell financial institutions a great deal that they did not already know about their IT outsourcing responsibilities in the cloud context.

In substance, the Statement affirms that outsourced cloud computing services are subject to the same basic risk identification and risk management principles and requirements that exist in the existing regulatory guidance.[6] The Statement goes on to say, however, that the nature of cloud computing services may require "more robust" controls.

And what are those controls? The Statement identifies six areas where financial institution risk management efforts relating to outsourced cloud IT services need to be particularly vigilant: (i) due diligence of cloud IT vendors; (ii) management of cloud IT vendors; (iii) vendor audit responsibilities; (iv) information security; (v) legal, regulatory, and reputational risks; and (vi) business continuity planning. Those financial institutions familiar with the Agencies' existing IT guidance on outsourcing in general will find nothing new in these broad areas, but the Statement does go on to highlight specific issues within these six areas that arise in the cloud IT environment.

Due Diligence: The Agencies expect financial institutions, through a due diligence review, to ensure that cloud IT service providers can meet the financial institution's requirements for cost, quality of service, compliance with regulatory requirements, and risk management. The Statement identifies the following specific areas that financial institutions should take into account, and review and evaluate, during the due diligence process:

- **Data classification:** the sensitivity of data that will be placed in the cloud and the controls that will be needed to ensure it is properly protected (e.g., encryption of non-public personal information and other data whose disclosure could harm the institution or its customers).

- **Data segregation:** whether the financial institution's data will share resources with data of other cloud clients, and the controls that service providers will have in place to ensure the integrity and confidentiality of the financial institution's data.

- **Recoverability:** the financial institution's and IT service provider's disaster recovery and business continuity plans.

---

[4] IT industry surveys point to the likelihood of a continuing significant migration away from "hard" IT platforms towards Internet-based services as a solution for hardware, infrastructure, and software needs alike. *See*, Pew Research Center, *The Future of Cloud Computing* (June 2010), *available at* http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx.

[5] IT Handbook, *Outsourcing Technology Services*, n.3 *supra*.

[6] "The fundamentals of risk and risk management defined in the IT Handbook apply to cloud computing as they do to other forms of outsourcing." Statement, at 4.

Vendor Management: The Statement generally cautions financial institutions to ensure that their cloud computing service providers are familiar with the financial industry, and the legal and regulatory requirements for safeguarding financial customer information and other sensitive data, and are able to address applicable regulatory requirements. Financial institutions, especially smaller ones, are also cautioned that cloud IT contracts and service level agreements must be "specific as to the ownership, location(s) and format(s) of data, and dispute resolution."

Audit: The Statement cautions financial institutions that they may need to adjust their audit policies and practices to provide acceptable IT audit coverage of outsourced cloud computing, and augment their internal audit staffs' resources with additional training as well as having personnel with sufficient expertise in evaluating shared environments and virtualized technologies.

Information Security: The Statement advises financial institutions that they may need to revise their information security policies, standards, and practices to incorporate the activities related to a cloud computing service provider, which may include "continuous monitoring" in high-risk situations. Financial institutions are also expected to maintain a "comprehensive data inventory and a suitable data classification process" and limit access to customer data through effective identity and access management, particularly in the case of multi-tenant cloud environments. The Statement also cautions financial institutions on the identification and management of data in the cloud, saying they should ensure effective monitoring of, responses to and investigations (including forensic strategies) of "security-related threats, incidents, and events" on both their own and their servicer providers' networks. The Statement specifically refers to the necessity to use caution in storing data in overseas locations, which may require financial institutions to place contractual restrictions on the locations at which providers may store data. In addition, the Statement advises financial institutions that it would be "prudent" to ensure that a cloud IT service provider is obligated, and has procedures in place, to remove all non-public personal information from its infrastructure at the conclusion of the servicing relationship.

***Legal, Regulatory, and Reputational Considerations*:** The Statement warns financial institutions that they should clearly identify and mitigate applicable legal, regulatory, and reputational risks, given the complexity of compliance with applicable laws and regulations in a cloud environment where customer data may be stored or processed at remote locations, including overseas. Financial institutions are expected to understand the applicability of laws and regulations within the hosting jurisdictions and the financial institutions' ability to control access to their data. Contracts with cloud IT service providers should address the parties' obligations with respect to compliance with privacy laws, responding to and reporting security incidents, and fulfilling regulatory requirements to notify customers and regulators of any breaches.

***Business Continuity Planning*.** Finally, the Statement cautions financial institutions to determine whether a cloud IT service provider and the network carriers have adequate plans and resources to ensure a financial institution's continuity of operations, as well as its ability to recover and resume operations if an unexpected disruption occurs.

Some Observations

The Agencies' Statement, like the existing FFIEC guidance on IT outsourcing activities in general, is principles-based and short on specific requirements for risk management and compliance strategies, policies, and procedures. [7] Therefore, financial institutions will not find a great deal in the Statement that will materially aid them in meeting their supervisory obligations with respect to the procurement and use of cloud computing services from third parties, although the Statement might serve as a type of checklist of substantive issues that must be addressed. Part of the difficulty with the application of these agency guidelines to specific cloud IT

[7] Financial institutions may find more useful information in the IT Handbook sections that have been modified to address cloud computing issues, in particular Appendix A and Appendix D to the IT Outsourcing Handbook.

applications is that the nature and depth of the risk management issues, and the solutions to those issues, will vary significantly according to the type of cloud platform being used (public, private, hybrid), the nature of the applications being acquired (IaaS, PaaS or SaaS), and the nature and sensitivity of the information being placed "in the cloud."

What is perhaps more significant about the Statement is that it reflects a discrete level of regulatory concern over the risks specifically associated with cloud IT environments, particularly in areas such as vendor management, information security, data integrity and business continuity planning. These specific concerns may be less relevant – but not totally irrelevant – to financial institutions that employ private cloud networks, but any financial institution that proposes to use any type of shared cloud solution will need to be fully attentive to these regulatory worries. At a minimum, this would require the development and implementation of documented programs, policies and procedures to support a financial institution's selection and implementation of a particular cloud application, and demonstrate that the risks identified in the Statement have been specifically considered and addressed.

In addition, cloud IT vendors are effectively being told by the Agencies that they must "play ball" with their financial institution clients by addressing to the Agencies' satisfaction the particular legal, regulatory, and supervisory obligations of regulated financial institutions with respect to their IT procurement activities. Current experience, however, suggests that many public and hybrid cloud system service providers have not reached the point of fully accommodating the particular business and regulatory obligations of highly regulated financial institutions. In many such relationships, vendor terms and conditions are generally tilted in favor of the vendor on core matters (including service levels, business continuity responsibilities, rights of termination without cause, remedies for damages, and limitations on indemnifications). These vendors have typically been reluctant to negotiate away from these terms because their business models have depended on a "one size fits all" approach. However, given the Agencies' increased scrutiny over financial institutions' use of cloud-based solutions, IT services providers in the cloud environment that are disinclined to respond to financial regulatory concerns in areas such as audit, data protection and business continuity may in the future be left "outside the gates" of the financial institution community.

In sum, the Statement adds little of substance to the task of addressing and resolving the known technology, operational, legal, and regulatory issues associated with cloud technology.[8] At the same time, the Statement serves as a cautionary note that the Agencies will be attentive to whether their regulated financial institution constituents properly address and resolve these issues before they enter into a third-party cloud IT relationship.

Author

Charles M. Horn
(202) 887-1555
charleshorn@mofo.com

[8] In prior publications on cloud computing activities, we have highlighted several major issues that are particularly associated with cloud computing activities, including privacy, data security/integrity, TSP negotiation issues, and how users of cloud services may need to approach these concerns. *See*, Morrison & Foerster LLP, *Privacy in the Cloud: A Legal Framework for Moving Personal Data to the Cloud* (Feb. 14, 2011); *Cloud Computing and Outsourcing: Is Data Lost in the Fog?* (June 15, 2009); MoFoTech Magazine (Supplement), *Get Your Head in the Cloud* (2010).

Contacts

Financial Services

Rick Fischer
(202) 887-1566
lfischer@mofo.com

Oliver I. Ireland
(202) 778-1614
oireland@mofo.com

Andrew M. Smith
(202) 887-1558
andrewsmith@mofo.com

Barbara R. Mendelson
(212) 468-8118
bmendelson@mofo.com

Technology Transactions

Chris Ford
(202) 887-1512
cford@mofo.com

John F. Delaney
(212) 468-8040
jdelaney@mofo.com

About Morrison & Foerster

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life sciences companies. We've been included on *The American Lawyer*'s A-List for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.