FOX ADVISORS
An Accountancy Corporation
Pacific Center
701 Palomar Airport Rd, Suite 300
Carlsbad, CA 92011

The Cloud and Internal Control

October 2011

**By Frank E. Fox CPA/ABV/CFF/CITP, CFE and Susan A. Fox CPA/CFF, CFE
Principals, Fox Advisors**

The Cloud has made it easy for companies to outsource and access the full spectrum of business-related applications and tools, from file management to ERP to human resources; use of the Cloud enables companies with limited budgets to obtain IT-related services.

The National Institute of Standards and Technology, a non-profit organization that develops standards to ensure adequate information security for federal agencies (and whose standards may be used by non-governmental organizations) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

There are three models in cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS enables users to run software, and the user does not control the cloud infrastructure, but does have control over operating systems, storage, and applications. PaaS enables users to deploy their own applications (whether acquired or created) onto the cloud infrastructure, but users only have control over their own applications; users have no control over network, servers, operating systems, or storage. SaaS provides users the ability to use the provider’s applications in a cloud infrastructure, and users have no control over networks, servers, operating systems, or storage.

Cloud services are deployed using one of several models: public, private, community, and hybrid models. Public clouds are made available to the general public or industry groups, and the cloud infrastructure remains with the Cloud Service Provider (CSP). Private clouds are made available solely to specific organizations, community clouds are developed for use by a specific community of users, and hybrid clouds are a combination of public, private, or community clouds. Private, community, and hybrid cloud infrastructures may or may not be managed and operated by the organizations or communities themselves.

Because your company may have no control over the operating infrastructure in the Cloud, it is important for you to implement controls to mitigate some of the data security risks inherent in cloud computing.

In addition, data processing and/or storage in the Cloud are decentralized. Make no mistake – this lack of physical access to servers, as well as knowledge about where your company's data may be located, currently makes it difficult, if not impossible to fully secure private or sensitive corporate data. You can take steps, however, to ensure that you have been as diligent as possible in monitoring controls **around** the Cloud.

Your decision to move your company's data to the Cloud not only has operational implications; it has legal and compliance implications as well. For example, if your company becomes a party to a lawsuit, you may be obligated to produce electronically stored information (ESI) for your case. If all of your data is stored in-house, you have control over all information, applications, data, computing, and storage; you lose that control if you're using the Cloud, and may be forced to rely on your CSP to produce data for litigation purposes.

There has been some litigation already involving such data requirements, and it's logical to assume that responsibility for ESI to be used as evidence in a lawsuit lies with a company's management. One solution is to negotiate with your CSP to ensure that you have ready access to all ESI maintained by your CSP. Another solution is to work closely with your company's IT department to carefully define user-specific application configuration settings when you first move to the Cloud.

Compliance issues also result from a move to the Cloud. The lack of control mentioned earlier makes it difficult to adhere to SOX requirements, but there are a few solutions. You may want to answer the following control questions in conjunction with Entity Level testing at your company:

1. Does Corporate Counsel have an intimate understanding of the company's business and IT strategies in this area, particularly the nature of the company's cloud infrastructure?
2. Does Corporate Counsel/IT document the location of servers used for cloud computing (i.e. the storage of information on servers in countries with fewer legal protections for ESI)?
3. Does the Company have a policy or procedure to address specific issues and possible concerns relating to the potential theft, loss, or disclosure of confidential information stored in the Cloud? These issues and concerns include:
    - A vendor's failure to back up data adequately, including ensuring redundancy.
    - The ability to access corporate data using easily accessible software in the event that the corporation terminates its relationship with the cloud computing provider or the provider goes out of business.
    - The provider's procedures for responding to (or when appropriate, resisting) government requests for access to information. What if, for example, a government (domestic or foreign) seizes the actual servers (i.e. hardware)?

Without guaranteed redundancy, the Company may have no recourse and may suffer serious consequences.

- Insufficient data encryption.
- Unclear policies regarding the corporation's ability to "control" its own data, which may result in problems if served with a request for production of materials under Rule 34 of the Federal Rules of Civil Procedure.
- Policies for data destruction when the corporation no longer wants the relevant data available or transfers it to a different host.

4. Has Corporate Counsel or the Company's management conducted due diligence on all cloud vendors and negotiated terms and conditions governing the stewardship of its data?
    - Ensure that your online data provider has an enforceable obligation to preserve confidentiality and security, and that it will notify you in the event of any security breach (defined as broadly as possible) or if served with process that in any way relates to your data.
    - Investigate the cloud service provider's security measures, policies, recoverability methods, and other procedures to assess security adequacy.
    - Ensure that said vendor is using the most appropriate technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.
    - Ensure that the cloud service provider can "purge and wipe" any copies of the data and move it to a different host if necessary.

Finally, it's essential that Cloud users understand the following important fact: as a Cloud user, your data will likely be stored on multiple servers – servers that you may share with other Cloud users. Because your company may share server space with other companies, your company's data will only be as secure as the other companies who share server space with you in the Cloud. Whenever possible, consider negotiating with your CSP for a dedicated server, to ensure that your company's data does not reside on the same servers with other Cloud users.

Speak with your CSP as well to determine what the CSP is doing to keep your company's data secure. In the event that your data resides on a shared server, ask your CSP to outline the steps it plans to take to maintain your company's data security in the event that another company's data on that shared server must produced for legal or other purposes.

The above recommendations are just a start; we will continue to provide more information about internal control in cloud computing environments as cloud computing continues to mature.

Frank E. Fox and Susan A. Fox are principals with Fox Advisors, Inc. The firm provides corporate governance, business valuation, and forensic accounting services, as well as IFRS-related consulting (www.foxadvisorsinc.com).