

In Perspective

McQuade.Brennan.LLP.

Certified Public Accountants and Consultants

Uniquely built to exceed your expectations

[Home](#) [Our Firm](#) [Tax Forms](#) [Tax Calendar](#) [Contact Us](#) [Brian's Blog](#)

Cloud Computing

Understanding the Risks of Cloud Computing

Cloud computing is helping to reshape the information technology landscape. It may also be injecting considerable operational risk that may not be readily understood or appreciated by business owners and executives.

The Basics of Working in the Cloud

Instead of installing software or hardware within the company's information technology infrastructure, cloud computing allows companies to access a shared pool of data resources using web based applications. Cloud computing can be managed three ways:

- **Software as a Service or SaaS** - Software and data resides within the service provider's environment. Data is accessible via most web based portals. Data back-up and security protocols typically reside with the service provider. (This is sometimes called "on-demand software.")
- **Platform as a Service or PaaS** - Provides users access to a development platform where the development tool resides on a third party server.
- **Infrastructure as a Service or IaaS** - A company uses a third party's information technology infrastructure, including storage, hardware, and servers. (This is sometimes called "hardware as a service.")

Key Cloud Computing Issues to Consider for Your Business

1. Estimate the impact of a platform failure

A company should estimate the cost of a cloud platform failure and how to prepare for it. Preparing for a failure requires an additional investment and your company should prepare an estimate of how the failure could impact its financial performance.

Some companies build their cost estimates on a per-minute basis. Most cloud computing providers provide a service level commitment as a percentage of the year. If a cloud computing provider states that their service level commitment is 99.99 percent, which translates to data being unavailable for 53 minutes each year. What is promised and what actually occurs can be drastically different.

The cloud computing provider should also frequently back up your company's data. Your company needs to make sure processes are in place to back-up data on a daily basis and how new data will replace or build upon old data.

2. Ensure data availability

Before data is moved to the cloud, make sure you have an agreement on data availability documented in a service level agreement (SLA). The SLA should include the associated penalties if data becomes unavailable. The penalty for breaching the SLA is typically specified by the cloud computing service provider. However, depending on the number of cloud

Personal Info
Saved Articles
Calculators
Unsubscribe
Feedback

Your Privacy

© 2011, Powered by BizActions

computing users in your company, it may be possible to negotiate a significantly higher penalty.

3. Develop a back-up plan

It may be worthwhile to invest in a "back-up cloud" in case the primary cloud fails. Alternatively, it may be possible to revert to your company's existing infrastructure. Ask your cloud provider to share their contingency plan in the event that a cloud data center fails.

4. Research insurance options

Your insurance carrier may be able to provide insurance coverage for cloud outages. The expense may be justifiable if the anticipated financial impact of a cloud failure is in excess of the annual insurance premium.

Cloud computing typically provides a far more flexible solution than traditional information technology infrastructure as well as significant cost savings. Since the cloud computing customer does not own, manage or control the infrastructure, researching an insurance option would be a smart decision before switching to a cloud.

5. Educate employees

Once data resides in the cloud, employees will be able to access company data wherever there is an internet connection. Staff members need to be educated about the dangers of accessing company data in public places, such as coffee shops, airports, or internet cafes. This is just as important as reminding employees to protect their company network log-in credentials. Special attention should be given to "phishing" e-mail messages that routinely trick employees into providing their log-in information and passwords. Phishing e-mails may appear to be from the cloud company's administrator when they are actually fraudulent.

6. Keep informed of evolving cloud computing legal issues

The legal environment often takes time to catch up and provide definitive guidance with the introduction of new technology. As costs continue to decrease and more companies migrate their data to the cloud, the pace of legal requirements will likely increase. Consult your attorney about staying up-to-date on cloud-related legal developments.

 [Email to a Friend](#)  [Save Article](#)  www.mcquadebrennan.com  [Share This](#)

Feedback

- Is this item worthy of implementation? Yes No Maybe
- Is this item worth sharing with other associates? Yes No Maybe
- Did this item present value to you and your business? Yes No Maybe

Comments: