How to Avoid Turbulence When Moving Operations to the Cloud

By Alexis Kennedy, CPA, CISA, CISSP, CCSFP

In Texas, heavy clouds can bring much-needed rain, but they can also build into thunderstorms and tornadoes, creating havoc in their path.

In the same way, doing business in the cloud offers enormous benefits, including cost savings, increased information security and scalability. At the same time, there are also risks, including mishandling of private company data, lack of availability of key business functions and challenges in controlling levels of spend.

In the simplest terms, cloud computing means storing and accessing data and programs over the internet instead of on a computer's hard drive. When information is stored in the cloud, it means it is stored on a server managed by someone else rather than on a server managed within your walls. Cloud service providers are third-party companies that offer a cloud-based platform, infrastructure, application or storage.

For many organizations, transferring certain computer-based operations to the cloud by engaging a cloud service provider offers operational and cost efficiencies. Outsourcing an area that may not be an internal core competency may actually reduce information security and privacy risks.

As with any third-party relationship, the devil is in the details. Organizations need to perform proper due diligence, negotiate contracts that specify explicit responsibility matrices over ownership and ultimate responsibility for data that resides within the cloud platform and make sure they have a process in place for ensuring that service providers are meeting their contractual obligations.

For organizations that are considering transferring some aspects of their operations to the cloud, the key is understanding that engaging a cloud service provider does not mean 100% of the organization's risk is transferred to that provider. Organizations that do business in the cloud are still responsible for assessing and addressing these risks. That's why they need to adopt and follow comprehensive internal cloud management procedures, as well as procedures for monitoring their service providers.

Making the Move

Moving business to the cloud is not as easy as just flipping a switch. Before any decision is made, there must be ample research and consensus within the organization. The cost implications, including the shift from capital intensive outlays to recurring operating expenses, must be modeled out with the chief financial officer.

Alignment of the organization's customer service levels with the service levels provided by the cloud service provider must be reached with legal, sales and customer success departments.

In instances of internally developed applications, software architects must be engaged to determine whether the architecture of the application will perform as expected in the cloud. Cybersecurity and risk

management functions must also be engaged to address changes in the risk landscape.

Selecting the Right Type of Service

The first step is to evaluate and select the type of service that best meets the needs of the organization. Of many different options currently available, these are the three most common kinds of cloud service providers on the market today.

Infrastructure as a Service (IaaS). IaaS provides access to networking features, computers (virtual or on dedicated hardware) and data storage space. Flexibility and scalability are its major benefits. In a sense, this is a form of outsourcing an organization's IT asset management.

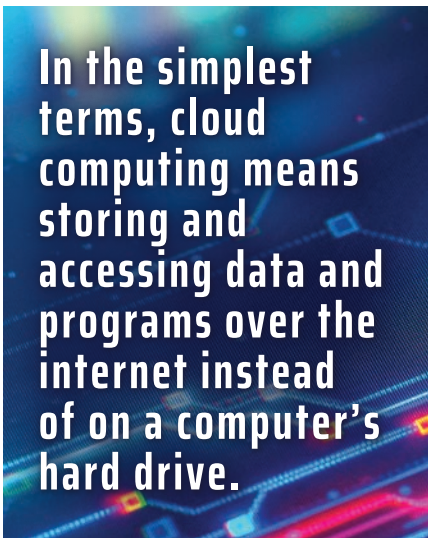
With a third party owning and managing the infrastructure, it can be easier to add capacity and grow quickly with a smaller capital investment. IaaS is typically very accessible and can support an organization's disaster recovery and business continuity objectives.

Platform as a Service (PaaS). This level of service provides organizations with full management of the infrastructure supporting the applications, which allows the organization to focus on developing and deploying applications for its business.

In a PaaS environment, the organization only needs to provide its code. The service provider manages the underlying infrastructure, including patching, software management and capacity planning.

Software as a Service (SaaS). SaaS provides a fully developed and deployed application or product. Once deployed in the cloud, this application is usually managed entirely by the service provider. Maintenance of the underlying infrastructure, as well as the development and maintenance of the application, are typically all part of the outsourcing agreement.

A SaaS platform can help reduce the number of application developers an organization needs to employ while increasing the availability and scalability of the application.



Selecting a Provider

Once an organization has determined the appropriate type of cloud service, the next step will likely be selecting an outside service provider. The main goal is for the organization to understand potential risks of engaging with a service provider and to have an understanding of how the service provider manages its business risks. In this way, the organization will be able to better anticipate the impact to the organization of outsourcing certain risks.

Assessing and managing risk can be challenging since significant portions of the service environments are under the control of the provider and may likely be beyond the purview of the acquiring organization.

However, it is important for the organization to perform due diligence up front to assess the risks associated with engaging a service provider. The organization must be able to answer these questions:

- What services are being outsourced?
- What business processes will be supported by the service?
- What data will be stored, processed or accessible via the cloud service?
- Where will the data be stored and processed? (This is important when dealing with contracts that restrict where customer data can be stored or processed.)
- Who will have access to systems, applications and data related to the cloud service?

A service provider pre-assessment form can be used to gather preliminary information from a potential service provider. Common questions in a supplier pre-assessment form include:

- Has your company ever declared bankruptcy?
- Does your company's insurance policy include errors and omission (or general liability) claims? If yes, what are the limits of the policy?
- Is your company involved in pending litigation?
- Has your company ever been a party to a regulatory investigation?
- Does your company have a privacy policy?
- Does your company have a documented information security program in place?
- Will your company agree to complete a questionnaire regarding your information security and privacy programs?
- Will your company allow for the audit of your organization's security controls?
- Does your company have a Service Organization Controls (SOC) report or other third-party security attestation such as ISO 27001, HITRUST, PCI?
- Does your company have a comprehensive business continuity plan to address continuance of operations in the event of incidents disrupting normal operations?

These assessment forms should provide sufficient information to determine whether additional diligence is needed. Based on the level of potential risk, this additional diligence could include requiring the service provider to respond to a more detailed questionnaire, reviewing the service provider's SOC report in detail or engaging with the organization's internal audit function or a qualified external audit firm to conduct a vendor assessment.

Engaging a Provider

Once due diligence is complete, the organization is ready to engage a service provider and begin implementing its services. Before doing so, however, both parties must have a clear understanding of the security responsibilities of both the organization and the cloud service provider.

Typically, the service provider is responsible for security of the cloud (the network, computer and storage layers) while the organization is responsible for security inside of the cloud (the applications and data). Ideally, a responsibility matrix that specifies these responsibilities should be embedded in the contract with the provider.

In the Cloud, Now What?

Due diligence should not end with the signing of the contract. The organization must continue to monitor its outside service provider for overall performance and adherence to contractual obligations.

This monitoring should include regular reviews of invoices to understand the expense characteristics of the solutions moved to the cloud, ongoing assessment of service availability and recurring assessment of the security profile of the migrated solutions.

One of the most efficient ways to perform an annual review of the provider's adherence to committed operational processes and procedures is to request and review the provider's SOC report. SOC reports include a great deal of information and can be challenging for organizations to review. But they can be useful in determining whether the outside service provider is adhering to its contractual obligations.

The contents of the SOC report should reflect the specific needs and risks of the organization. Test procedures should define the extent of testing performed to give reasonable assurance over the operating effectiveness of the controls.

In reviewing a vendor's SOC report, the organization may identify a weakness, either through the service auditor's identification of a deviation or through the organization's perceived gap in the control environment. In these cases, the extent and exposure of the particular gap should be evaluated.

It's important to keep in mind that not all SOC reports are created equally. A reputable, experienced and knowledgeable CPA firm should perform the SOC report. In addition to the results of the auditor's testing, the organization should pay specific attention to the "complementary user entity controls" section of the SOC report. To ensure that the controls reported on in the cloud service provider's report will operate effectively, this section specifies the organization's responsibility within its own control environment.

These considerations should not be news with the issuance of the report, as these responsibilities should have been discussed and agreed upon during the contract negotiations. If they were not, the organization should ensure that it has the controls in place to address the applicable complementary user entity controls.

If a SOC audit or equivalent attestation is not available, organizations should pay particular attention to:

- How the service organization/vendor provides transparency to their internal control environments to ensure expectations are being achieved, and
- How beyond inquiry, the service organization/vendor can convey consistency and reliability on that internal control environment.

As more and more organizations move parts of their operations to the cloud, following these steps will be critical for success. The ride may be bumpy at times, but in the end organizations that put in the effort on the front end are more likely to capture the many benefits and efficiencies gained by working in the cloud.

About the Author:

Alexis Kennedy, CPA, CISA, CISSP, CCSFP, is a Senior Manager in IT advisory services for Weaver, a Texas-based national accounting firm. She has consulted with a wide range of clients on security compliance, and performed and led IT audits across multiple industries and technology platforms.