TECH Practices

By Jim Scott, CMA

Mitigating Risk When Migrating to the Cloud

The Swiss investment banking company UBS AG recently released a survey of chief information officers of the top 100 companies in the United States and Europe. More than half the respondents plan to migrate some internal information technology (IT) functions to the public cloud. One-third said they are already in the process of moving to the public cloud as quickly as possible. A majority of companies have already moved some of their applications to the cloud. Add in the rapid growth of Software as a Service (SaaS) applications and the efforts of IBM, Microsoft, and others to join Google in the public cloud, and these signs clearly point toward the cloud environment being both the preferred present as well as the likely future for storage, e-mail, applications, and management systems.

A Risky Environment

Migrating to the public cloud has its own risks, and living in the cloud has many of the same service risks a company already faces. It's generally agreed that the cloud offers better availability, reliability, and security than most companies can provide on premises. This is especially true for small and medium-sized enterprises (SMEs), where dependence on outside service providers and limited in-house staff have long been the norm. Many people will argue that cloud security is better even for large enterprises that now run their own dedicated data center.

The challenge for management accountants is to understand more about the cloud in order to create the reporting necessary to demonstrate a return on investment (ROI) so that companies can make the proper choice when it comes to deciding on cloud vs. on-premise or managed colocation solutions or which cloud offering is best. Often the proposed solutions are devised by IT with the help of some very hungry vendors.

Needless to say, be wary of any ROI models proposed by a vendor. It's very unlikely that the reality will ever replicate the modeled results offered. Any proposed labor savings are elusive because it usually doesn't take fewer people to manage cloud services. Internal support for cloud services is the norm, on top of the services provided (usually at an additional cost) by the vendor.

The private cloud solution(s) pursued by some companies usually become hybrid clouds at some point. Like it or not, most company users delve into the public cloud for some applications with or without company approval. The cloud shares many of the traits of a traditional IT environment, and the need for security is the same in many ways.

Secure Your Information

The three primary security objectives common to all IT systems should be addressed when choosing a cloud services provider or evaluating a move to the cloud. They are confidentiality, integrity, and availability.

Almost every company can greatly improve physical security by moving from an on-premise environment to a secured Tier III data center. Multiple levels of security stand between the outside world and the equipment itself. Perimeter security, guards patrolling 24/7, biometric scanning, badging and security checking, multiple locked areas with controlled keycards, and monitored security cameras all come standard. These data centers also have far superior data and power connections, usually involving multiple power grids, continually monitored and tested generator backups, and multiple Internet service providers with huge and redundant bandwidth. Assuming your equipment is on-premise now, the cloud provider itself usually is much more secure, but be sure to investigate any SaaS or cloud service provider to determine what data center they're using and what standards that center operates under. Or if they're serving the public cloud from their own dedicated center, ask whether they are Tier III certified by the Uptime Institute.

Pitt Turner, executive director and senior tier certification authority with the Uptime Institute, said, "Tier III Design Certification signifies a design solution that is capable of responding to a 24 × 7 performance objective—without shutdowns for equipment work or replacement." Tier III data centers are certified as having multiple power and data paths in place to serve the IT equipment itself. This addresses the availability concern (nothing beats 24/7 service and the service-level agreement guarantees of most cloud service providers).

The Salesforce public cloud SaaS customer relationship management (CRM) provider is very transparent about the use of third-party data centers owned by Equinix, which operates Tier III-certified data centers. In addition to Salesforce, Equinix also serves Etsy, Box, and Priceline. (Letting others validate your service provider's choice of data center is one way to accelerate your due diligence.) Salesforce provides continuous monitoring so that every customer can see the status of the data. You should expect similar reporting from your cloud service provider.

Assuming your cloud service provider's data center is Tier III certified, the next step is to ensure SSAE (Statement on Standards for Attestation Engagements) 16 certification. SSAE 16 has replaced SAS (Statement on Auditing Standards) No. 70 Type 1 and Type 2 audit reports. SSAE 16 Type 2 ensures that integrity and confidentiality are maintained by the provider. Part of testing is to ensure proper backups, endpoint security protocols, and segregation of customer data. The audit includes internal controls, procedures, and processes. Most data centers and providers can provide this audit and advertise it as a selling point on their websites. A Type 1 report is limited to a review made at one point in time and covers the design effectiveness of internal controls only. Type 2 is a more thorough analysis that covers at least a six-month time period and measures the effectiveness of the operating internal control plan in place. Some providers may not be in operation long enough to have a Type 2 report, but any long-established provider should be able to either provide this or give assurances that a Type 2 audit is under way.

The First Step

The first consideration when evaluating a migration to the cloud is the physical and systemic security of the provider chosen. Following this guide will help you determine a minimum of what you need from your cloud services provider.

But your job isn't complete. Once these basics are in place and your cloud services provider has demonstrated a secure physical environment, service availability, and attention to effective internal controls that ensure confidentiality and information integrity, you can begin to address the confidentiality, integrity, and availability of information within your own company and users. This can involve the challenge of securing every device and network that connect to your cloud services provider. And to support the highly mobile business world, other operational factors and considerations need to be addressed, such as encrypted data storage and transfer, multifactor authentication, password ratings, and antimalware software. Management accountants need to be conversant with and knowledgeable about these basic security issues. **SF**

Jim Scott, CMA, is CFO and COO of TetherView. He is a member of the IMA® Technology Solutions and Practices Committee and a member of IMA's North Jersey Shore Chapter. You can contact Jim at thecfo@outlook.com.