The most frequently used technology phrases in recent history have stemmed from the proliferation of cloud services. Service providers are developing and relabeling services to capitalize on the attention and movement to the cloud as a method to outsource processes, maintain technological advantages and reduce costs. Cloud service offerings have grown exponentially and continue to gain traction because of the promised benefits that cloud computing delivers.

Many companies are now selecting hosting providers that offer infrastructure in the cloud for their customers. These companies reap the benefits of access to advanced technology at a fraction of the cost of making capital investments in dedicated systems. Shared services can deliver improved capabilities to multiple clients who make a shared investment in the technology. However, many of the users of these systems assume that they are outsourcing risk to the cloud as well. I call this “security by abdication.” Security by abdication is when a company decides that rather than accept the responsibility of securing and maintaining systems, people or processes, it will abdicate the responsibility by moving to the cloud.

**OUTSOURCING RISK?**

During an audit, we often hear the phrase, “they handle that.” In other words, the company has signed an agreement for Software as a Service or Infrastructure as a Service and breathes a sigh of relief because its responsibility for security on those systems is supposedly in the hands of the service provider. In actuality, the company’s responsibility for governing security has not been removed, it is merely different, and must be evaluated in the context of the cloud service, the cloud provider and the purpose for which the company is utilizing the service.

American Health Centers Inc. (AHCI) is an example of an organization that chose to outsource its critical infrastructure function, choosing independenceIT, a cloud IT vendor. The AHCI risk assessment determined that the benefits of hosting data in a secure off-site data center would outweigh the risk of outsourcing management of the systems. It also determined that, given proper governance, security would be improved because the monitoring of access controls provided by independenceIT was at a level that AHCI would not have been able to provide itself. Security governance is problematic for companies that do not wish to absorb the various matters that must be considered when evaluating risk and managing security.

For a company in the business of, for example, producing widgets—and not in the business of securing systems, applications and people—the security function is overwhelming, to say the least.

**OVERSEEING SECURITY AND GOVERNANCE**

It has been difficult to ask senior executives to oversee a topic with which they are uncomfortable because of the rapid changes taking place with technologies and persistent risks. Governing other departmental goals and objectives is more natural for business leaders and audit committees. Overseeing an information security program that permeates every department and requires a grasp of rapidly transforming subjects has not been as easily adopted.

Many organizations have appointed an information security officer or a different position to oversee the security function and report back to the board of directors. This arrangement has been generally accepted as satisfactory governance even while security incidents are on the rise in the corporate environment.

While governing the risks that it faces, AHCI chose to oversee independenceIT as a service.
provider by analyzing its risk management results and audit findings to evaluate the effectiveness of control mechanisms that protect the data and restrict access by unauthorized parties. Whether AHCI built and maintained the technology itself or outsourced the capability to independenceIT, AHCI still has an obligation to govern the information security program that will safeguard patient data.

It is important to note that many organizations’ current information security programs do not adequately address outsourced services because the expertise or ability to assess the risks associated with an outsourced provider have not been considered.

CHOOSING A COMPLETE CLOUD VENDOR
The business reasons for choosing a cloud services provider are clear. AHCI was able to provide its employees with cutting-edge technology and remote access to applications by using independenceIT’s remote desktop client, Freedom Desktop, thereby reducing the investment in processing speed and memory requirements. Additionally, the promise of managed security for these remotely accessed systems, applications and data means that the company will not have to monitor, update and test systems on a regular basis, as it would if it were managing all of the systems itself.

However, organizations must consider several other factors when choosing a cloud vendor. Without proper governance of the cloud service provider, an information security program is incomplete, major risks are not considered, and breaches will continue to occur due to misinformation or false expectations placed on the cloud service provider.

Governance of any service provider should include monitoring its risk assessment results to evaluate whether or not its policies and procedures are comprehensive enough to identify threats to its systems, physical locations, employees and vendors. A closer look at a service provider’s risk assessment and audit program discloses the matters that should be known by a customer using its services to host and manage sensitive data.

Finally, organizations should also review a vendor’s service organization control report because it details the provider’s risk assessment process, the controls it has placed in operation and the third-party tests performed to report on operating effectiveness. An organization must accept the responsibility of governing its service providers and what they provide to the company.

CONCLUSION
When outsourcing to a cloud vendor, all of these risks must be evaluated, and governance must be properly implemented, without the assumption that the cloud service is actually doing what it has promised. Due to the rapid expansion and adoption of cloud services, governance is needed more than ever to control and manage the risks.

Many organizations’ current information security programs do not adequately address outsourced services.

Enjoying this article?

• Read IT Control Objectives for Cloud Computing. www.isaca.org/ITCOCloud


• Consider attending ISACA’s Information Security and Risk Management Conference in Las Vegas, Nevada, USA; San Juan, Puerto Rico; or Barcelona, Spain, where there will be multiple cloud-related sessions. www.isaca.org/isrm