Managing Data Governance in a Cloud-Focused World

By Narjit Aujla, Manager – Data Management and Advanced Analytics

The rate at which companies are amassing data is staggering. More than half of organizations today (57%) have production workloads running in the cloud and with the amount of new devices being introduced that create, consume and transmit data to the cloud, it has become critical to have some type of cloud governance program in place. However, one of the most challenging elements of such a program is how to manage an organization's sensitive data. This data could encompass anything from bank account and credit card numbers to HR payroll data. Misuse or negligent handling of this information could cost companies tens of thousands of dollars *per record* lost in a potential data breach. Besides monetary consequences, we've also seen how disastrous a data breach can be to customer confidence. Cloud governance is nothing to scoff at!

When the stakes are this high, it is understandable that companies are reluctant to trust the cloud. Gartner predicts that "through 2020, 95% of cloud security failures will be the customers fault." However, cloud providers have made significant improvements to their security offerings over the last five years. This means that with proper planning and preparation, you can still reap the benefits of cloud efficiency and agility while maintaining appropriate levels of security.

Cloud Classifications

The types of cloud services on the market today can be classified into two categories: enterprise and consumer. An enterprise cloud service is one that meets current standards for security, application management and level of integration. Microsoft leads the field, delivering five of the top 20 most-used enterprise cloud services with products such as OneDrive, Exchange Online, SharePoint Online and Skype for Business. Consumer cloud services include popular social media sites such as Facebook, LinkedIn and YouTube. These services rely heavily on cloud infrastructure to deliver massive amounts of content on a global scale, a characteristic organizations may not consider when sharing their sensitive data. What's important to note from a governance perspective is that, compared to enterprise cloud services, consumer cloud security is lacking with only five percent of the top 20 services offering enterprise-grade security.

As organizations prepare to create new governance policies, it is helpful to understand what types of cloud services are currently being used across the company. A log analysis tool such as Splunk Enterprise Security identifies commonly used services and uses those statistics to create meaningful policies and procedures. According to Skyhigh Networks' 2016 *Cloud Adoption and Risk Report*, the most commonly used services in the market today can be grouped into three categories:

1. Approved services (5.4 percent of services) – these are services fully sanctioned by IT for having enterprise grade security and functionality and are often purchased and deployed at companies.
2. Permitted services (63.3 percent of services) – this category includes services that offer significant business value, but may require some risk mitigation strategies such as data loss prevention measures, activity monitoring and access control.
3. Not allowed services (31.3 percent) – includes services that are deemed too risky for corporate use. Examples might include online PDF converters and consumer-grade cloud storage providers.

Between Tradition and Trends

Organizations just beginning to use cloud solutions are often surprised to learn it is still possible to handle data governance like a traditional computing system. Tried and true elements of classical data governance such as a company charter, RACI matrix and data steward structure can be integrated and enhanced to incorporate the nuances of cloud workflows. However, because of how the cloud can change the way a business operates, it is strongly encouraged that organizations review existing policies to determine whether an existing policy can be enhanced or if a new policy should be created in its stead.

In a pre-cloud world, a company would likely be separated into three main functional areas: business, operations and IT. Now, cloud management responsibilities can span all three areas, which can essentially make it easier for lines of business to procure their own solutions and might necessitate the creation of a cloud management department and a restructuring of responsibilities:

- Because cloud infrastructure is a pay-for-service model, usage can be billed directly to a department. This will require IT to function as the broker of services rather than provider.
- Addressing the skill gap will either require training initiatives for existing employees or hiring of cloud architects to facilitate adoption, development and maintenance.
- Directors and managers of the organization will be involved in assessing the risk of migrating a particular system to the cloud. They will also be responsible for communicating with other departments and overseeing the adoption of new governance policies and workflows.
- Network and application security models must be enhanced to handle both on-premise and cloud infrastructure.

Integrating the cloud movement into an existing governance program is a crucial step in securing an organization’s data and optimizing new business processes. These considerations should help a data management organization plan ahead as it begins to adopt new and powerful cloud environments.