

Week 1 Assignment

William Slater

CYBR 615 – Cybersecurity Governance and Compliance

Bellevue University

The Roles of the Internal Audit Team in Cloud Computing

Ronald Woerner, M.S. - Instructor

December 2, 2012

Internal Audit's Role in Cloud Computing

The Internal Audit Team usually reports to an executive leadership level position and in every organization it has two primary responsibilities: 1) to ensure that the organization is in compliance with a framework of controls to for the purpose of managing risks in a consistent way, efficient, and cost effective manner; and 2) to ensure that the organization will meet the requirements to successfully pass audits conducted by external auditors.

A Brief History of the Modern Cloud and Cloud Service Models

In October 2005, Microsoft's Ray Ozzie and Bill Gates both published internal Microsoft memos that were purposely leaked to the press. These memos each described Microsoft's future direction to embrace and extend the idea of Cloud Computing. In fact, Ozzie made the statement, "People don't really care HOW this stuff works, they just want it to work. What followed was a technology race in which Microsoft decided to spend billions of dollars to design, build and operate "Cloud Data Centers" in a credible effort to compete with and perhaps even surpass Google, Yahoo, and Amazon.

In January 2008, after the publication of Nicolas Carr's book, *The Big Switch*, which outlined the business case for the sound economics and trend toward Cloud Computing, a veritable industry buzz started about Cloud Computing (Carr, 2008). This quickly led to the emergence of three commonly accepted general utility models of Cloud Computing as shown in the table below:

| Term | Explanation | Examples |
|------------------------------------|--|---|
| Infrastructure as a Service (IaaS) | Using Cloud Data Center Infrastructure to store data | Windows Live Skydrive, Backup, Storage, etc. |
| Software as a Service (SaaS) | Using provider-based applications located Cloud Data Center assets to perform business functions | Using GoogleApps, Yahoo Mail, Hotmail, etc. |
| Platform as a Service (PaaS) | Using the capabilities of Cloud Data Center assets to build customer applications that are designed for the Cloud. | Using Windows Azure and Microsoft Cloud-based components (SQL Server, Sharepoint, etc.) to build Cloud-based applications |

Table 1 – Summary of Common Cloud-Oriented Service Models

Since 2009, as businesses have begun to realize that migrating to one of more these Cloud Computing models could represent significant cost savings, Cloud Computing has become a predominant and disruptive paradigm shift, as important as the business adoption of the world wide web in the late 1990s and the client / server computing paradigm that took hold in the early 1990s (Rosenburg and Mateos, 2011).

Cloud Computing – Deployment Models

In NIST SP 800-145, the NIST terminology here, we see a shift to using ‘cloud’ to mean the a specific provision of cloud computing capabilities, rather than just as the network (Mell and Grance, 2011). The deployment models that are defined by NIST include the following:

| Deployment Model | Explanation |
|------------------|---|
| Private cloud | enterprise owned or leased |
| Community cloud* | shared infrastructure for specific community * sometimes called a “vertical cloud” |
| Public cloud | Sold to the public, mega-scale infrastructure |
| Hybrid cloud | composition of two or more clouds |

Table 2 – Cloud Computing Deployment Models (Mell and Grance, 2011)

Cloud Computing – The Evolutionary Trend

The diagram below shows the projections of how the trends will occur proportionately in the IT market from 2010 through 2030.

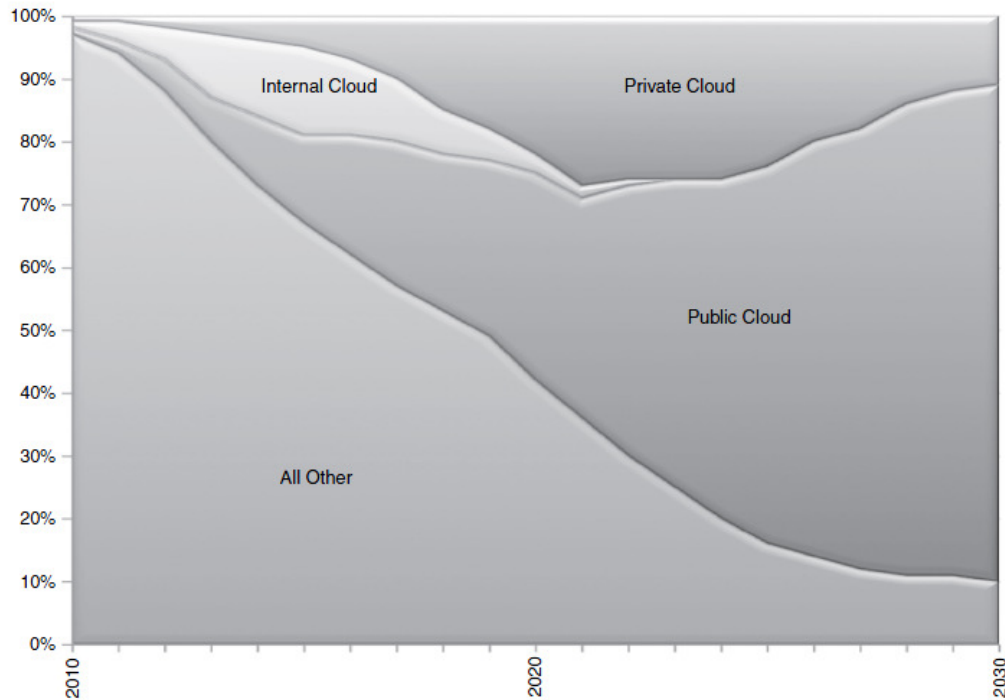


Figure 1 – Cloud Computing Evolution from 2010 – 2030, (Rosenburg and Mateos, 2011)

Cloud Computing – The Benefits

Besides the perceived cost benefits in cloud computing, there are several other compelling reasons that organizations consider migrating to cloud computing services. Among these are:

- Readily available access to Data Center resources and computing capabilities from practically anywhere, without have to own or maintain Data Centers
- Decoupling of business services and IT infrastructure
- Flexibility to choose from multiple vendors
- The elastic nature of computing resource usage where the user pays only for the computing services that they use
- Cost allocation flexibility; the ability to mode capital expenditures to operating expenditures
- Reduced costs due to operational efficiencies
- Faster deployment capability, from concept to design to deployment
- Operational risk reduction if contracts are properly constructed (Protiviti, 2012).

Security Issues in Cloud Computing

According to the Cloud Security Alliance, these are some of the biggest security concerns related to cloud computing services

- Abuse & Nefarious Use of Cloud Computing
- Insecure Interfaces & APIs

- Malicious Insiders
- Shared Technology Issues
- Data Loss or Leakage
- Account or Service Hijacking
- Unknown Risk Profile (Cloud Security Alliance, 2012)

According to the ENISA, these are some of the biggest security concerns related to cloud computing services

- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider (ENISA, 2009)

The Roles of the Internal Audit Team in Cloud Computing

The Internal Audit Team can play several roles in helping an organization move to one or more cloud computing models. Among these are

- 1) Helping build the business case for moving to cloud computing services

- 2) Selection of the right cloud computing service model
- 3) Selection of the right cloud computing service deployment model
- 4) Selection of the best cloud computing vendor
- 5) Ensuring that the organization remains compliant with its previously agreed security management frameworks
- 6) Helping plan and manage the implementation and/or migration to the cloud computing service model
- 7) Establishing the security controls framework for the new cloud computing services environment(s)
- 8) Monitoring the cloud computing service vendor and services for security, service performance, and all other contractually related issues.

Conclusion

As many organizations expect to trim IT staffs as a result of migrating to one or more cloud computing models, it is clear that the role of the Internal Audit Team will only increase in importance as organizations struggle with the challenges of successfully embracing various service and deployment models that are inherent in cloud computing. Without an Internal Audit Team to shepherd the actions of the IT and ensure that they remain compliant with the security management frameworks to which the organization has committed, the introduction of risk could be excessive and a real liability to the successful operation of the organization.

References:

- Carr, N. (2008). *The Big Switch: Rewiring the World, from Edison to Google*. New York, NY: W. W. Norton & Company.
- Cloud Security Alliance. (2011). *Security as a Service - SecaaS | DEFINED CATEGORIES OF SERVICE 2011*. Retrieved from https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf on October 24, 2012.
- Davis, C., et al. (2011). *IT Auditing: Using Controls to Protect Information Assets*. New York, NY: McGraw Hill.
- ENISA. (2009). *Cloud Computing Security Risk Assessment*. Retrieved from <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment> on December 1, 2012.
- Halpert, B. (2011). *Auditing Cloud Computing: A Security and Privacy Guide*. New York, NY: Wiley.
- Krutz, R. L. and Vines, R. D. (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. New York, NY: Wiley.
- Mather, T., et al. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. Sebastapol, CA: O'Reilly.
- Mell, P. and Grance, T. (2011). *The NIST Definition of Cloud Computing - NIST SP 800-145*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> on October 24, 2011.

- Ponemon Institute. (2011). Security of Cloud Computing Providers. A White Paper. Retrieved from <http://www.ca.com/~media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf> on December 2, 2012.
- Protiviti. (2012). The Role of the Internal Auditor in Cloud Computing. Retrieved from <http://www.knowledgeleader.com/> on December 1, 2012.
- Reese, G. (2009). Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. Sebastopol, CA: O'Reilly.
- Rosenburg, J. and Mateos, A. (2011). The Cloud at Your Service. Greenwich, CT: Manning.
- Winkler, J. R. (2011). Securing the Cloud: Cloud Computing Security Techniques and Tactics. Waltham, MA: Syngress.