Using COBIT to Manage the Benefits, Risks and Security of Outsourcing Cloud Computing

By Adesanya Ahmed, CGEIT, ACMA, ACPA

The persistent global economic challenges have compelled many enterprises to look for a way to restructure their business through the use of IT resources to increase productivity and efficiency and to reduce operating costs to increase in their return on investment (ROI). From general business improvements to strategic transformation initiatives, business executives are beginning to appreciate the fact that IT can be a powerful tool in helping to achieve their enterprises’ most important objectives. For example, IT can represent a core driver of cost savings for large-scale transactions across mergers, acquisitions and divestitures. In addition, IT is now a key interface between business enterprises and customers and has, thus, become the public face of the enterprise. Today, the use of IT can also enable the complete computerization of different business procedures, such as the supply sequence.

The innovative use of the Internet has enabled cloud computing to utilize existing infrastructures and transform them into services that the cloud could provide, resulting in both cost savings and increases in efficiency for an enterprise. By offering enterprises the opportunity to decouple their IT and infrastructural needs, cloud computing has the ability to offer enterprises long-term IT savings, reductions in infrastructural costs and pay-for-service models. By moving IT services to the cloud, enterprises can take advantage of using services in an on-demand model. With this system in place, less up-front capital expenditure would be required, thus, allowing businesses increased flexibility with new IT services. For these reasons, it is easy to see why cloud computing is an attractive potential service offering for any business looking for enhanced IT resources while controlling costs. However, there are also risks associated with the cloud, notably when using a third-party cloud computing provider. This article focuses on the benefits, risks and security of outsourced cloud computing and how COBIT can be utilized.

What Outsourced Cloud Computing Is All About

Cloud computing can be referred to as a dynamic way of attaining IT capability hardware, software or services from a third party over a network or through Internet technology. These cloud services are typically offered within a pay-as-you-go business model, and service types can include system and security infrastructure, application infrastructure and information, application, and business processes. This model allows enterprises to consume better services in the context of the business policy.

Some of the key business benefits offered by the cloud include:

- Faster entry into new markets
- Cost control
- Improvements in worker productivity
- Availability
- Resiliency

COBIT

In today’s complex business environment, management is looking for information to make difficult decisions on risks and control that would be quick and successful. Management wants to know the measures that should be taken and how to apply them. Enterprises need an objective way to know where they are and where improvement is required; they also need to be able to implement management tool kits to monitor this improvement. The answers to these issues are in COBIT. See figure 1.

COBIT is a comprehensive set of resources that contains all the information an organization needs to adopt an IT governance
and control framework. With this, enterprises can, thus, align COBIT with new technology.

**Risks and Security of Outsourcing Cloud Computing**

Many of the risks frequently associated with outsourcing cloud computing are not new, and they can be found in many enterprises today. Well-planned risk management activities will be crucial in ensuring that information is simultaneously available and well protected.

Business processes and procedures need to account for security, and information security managers may need to adjust their enterprises’ policies and procedures to meet the needs of the business. Given the dynamic business environment and focus on globalization, there are few enterprises that do not outsource some part of their business. Engaging in a relationship with a third-party cloud computing services provider will mean that the business is not only using the services and technology of the provider, but also must understand the way the provider runs its organization—the planning the provider has in place is its organizational culture and policies. In general, cloud computing acts as an accelerator for enterprises, enabling them to innovate and compete more effectively. With elastic and theoretically unlimited IT resources on tap, businesses no longer have to wait for the provisioning of servers or worry about project delays. They can quickly enter new geographical markets or launch new products or services in existing markets. As demand grows, they can quickly scale up. Conversely, when demand eases, they can just as quickly scale down and, if necessary, exit the market entirely with minimum loss of time and capital.

Risks involved in outsourcing cloud computing include:

- **Loss of governance**—Just as in traditional IT outsourcing, using the services of a cloud provider requires enterprises to give up control over their IT infrastructure. To make it easier for customers that take this step, cloud providers should make management and maintenance more transparent and auditable by customers. This should include recording logs and complete administrative sessions that affect the part of the cloud infrastructure used by customers, and, if requested, making these records accessible to customers. There must be strong authentication and authorization for the staff of the cloud provider and customers. This includes strong and possibly multifactor authorization methods, such as tokens or one-time passwords, on the one hand and strong authorization methods, such as 4-eyes authorization, on the other. Ideally, customers should be able to authorize and possibly monitor access to the system for the key systems they use. Such monitoring could be as simple as following the logs on an online interface or as sophisticated as watching a real-time audit trail of the administrator’s actions on the system—be it on a specific virtual machine or the hypervisor of the entire system. Allowing access to the audit trails of the hypervisor or providing 4-eyes authorization to customers may initially seem excessive, but it may be necessary for customers for compliance reasons.

- **Compliance**—Compliance requirements are becoming stricter almost every year, and a cloud provider that can meet these requirements and offer hard evidence of this compliance can gain significant advantage. Compliance usually covers the entire range of IT procedures, from system logging and log analysis to user and administrator authentication, authorization and auditing, but can also include data archiving, backups and recovery—not to mention the physical
security of the servers in the cloud. The trick here is to develop a system that can make the cloud compliant and that can prove the compliance of individual customers during an inevitable compliance audit.

- **Data protection**—Data protection and data abuse prevention are traditionally handled via authorization and strong access control and partly by using an intrusion detection system (IDS) and a data leakage prevention (DLP) system. Authorization can be handled by strong and possibly multifactor authentication, and access control and authorization can be enhanced by 4-eyes authorization methods. However, for obvious reasons, users must access a remote cloud using secure connections, which makes the use of IDS and a DLP system increasingly more difficult. Thus, a solution that can share the traffic of the encrypted channels with clients’ IDS/DLP system is highly beneficial.

- **Cloud provider selection**—Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks, except at extraordinary costs. Compliance with regulations and laws in different geographical regions can be a challenge for enterprises. At this time, there is little legal precedent regarding liability in the cloud. It is critical to obtain proper legal advice to ensure that the contract specifies the areas in which the cloud provider is responsible and liable for ramifications arising from potential issues. Enterprises could leverage the global compliance requirements that are becoming stricter and go for a cloud provider that can meet these requirements and is able to offer hard evidence of its compliance.

COBIT is a proven set of standards and processes that businesses can use to ensure that IT is working as effectively as possible to minimize IT-related risks and maximize the benefits of cloud. The security benefits of utilizing COBIT with the cloud include:

- **Customer compliance**—Connections from cloud customers using 4-eyes authorization to access a service running in the cloud (e.g., a Windows Terminal Service) can be audited. This can be useful if customers have specific compliance needs.

- **Selected authentication methods**—The use of selected authentication methods (e.g., certificates, passwords, public keys) should be enforced.

- **Customizable access control**—There should be strict yet easily customizable access control granted for users to have access only to selected log messages, e.g., messages related to the cloud services of a single customer.

- **Enforcement of 4-eyes authorization**—The enforcement of 4-eyes authorization with real-time monitoring and auditing capabilities effectively creates a strong auditing layer above the superuser layer accessing the devices, with the possibility to greatly increase the security of the cloud. For every security-aware customer, or for customers with special security needs, it is possible to require the representative of the customer to authorize cloud administrators, making the maintenance of the cloud’s infrastructure that is relevant to the customer completely transparent, auditable and reviewable.

- **Forensics and contracts**—Tamper-proof evidence for service level agreement (SLA) contracts and forensic situations should be provided.

**Conclusion**

While the promise of financial savings is an attractive enticement for outsourcing cloud computing, it is good to check compliance with the IT framework. Quite possibly, cloud computing is one of the best opportunities for enterprises to streamline processes and increase innovation. COBIT helps to document cloud computing ideal practices in a comprehensive, integrated manner and provides tools to measure, monitor and benchmark performance based on goals, metrics and maturity models. It also helps IT to show its value to the organization, and it easily integrates with and builds on other business and IT frameworks while improving their impact.
Adesanya Ahmed, CGEIT, ACMA, ACPA
is an IT security and connectivity consultant. He was the first to provide a broadband billing authentication for hotspot Wi-Fi and WiMAX Internet service providers (ISPs) in Nigeria. He can be reached at owos2001@yahoo.co.uk.

COBIT Focus is published by ISACA. Opinions expressed in COBIT Focus represent the views of the authors. They may differ from policies and official statements of ISACA and its committees, and from opinions endorsed by authors, employers or the editors of COBIT Focus. COBIT Focus does not attest to the originality of authors’ content.

© 2011 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Please contact Julia Fullerton at jfullerton@isaca.org.

Framework Committee
Patrick Stachtchenko, CISA, CGEIT, CA, France, chair
Steven A. Babb, CGEIT, UK
Sushil Chatterji, CGEIT, Singapore
Sergio Fleginsky, CISA, Uruguay
John W. Lainhart IV, CISA, CISM, CGEIT, USA
Mario C. Micaleff, CGEIT, CPAA, FIA, Malta
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, UK
Robert G. Parker, CISA, CA, CMC, FCA, Canada
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, Australia
Robert E. Stroud, CGEIT, USA
Rolf M. von Roessing, CISA, CISM, CGEIT, Germany

Editorial Content
Comments regarding the editorial content may be directed to Jennifer Hajigeorgiou, senior editorial manager, at jhajigeorgiou@isaca.org.