Cloud Computing: Overview and How to Audit

Dr.Lovepon Savaraj

Part-Time Lecturer of Thammasat Business School,
Thammasat University

บทคัดย่อ

Cloud computing is becoming more popular in the business world. Cloud services help organizations to reduce fixed information technology costs and scale business operations. Additionally, they support firms to access information easily and globally, and gain competitive advantage over other companies which have not yet leveraged the technology. However, although cloud services can lead benefits to organizations, they increase risk. This paper provides an overview of cloud computing——pros and cons, and how to successfully audit this technology.

Keywords: Cloud computing, Cloud services, Audit

การประมวลผลแบบกลุ่มเมฆ : ภาพรวม และวิธีการตรวจสอบ

ดร.ลัพธ์พร สวราชย์

อาจารย์พิเศษ คณะพาณิชยศาสตร์และการบัญชี
มหาวิทยาลัยธรรมศาสตร์

ABSTRACT

การประมวลผลแบบกลุ่มเมฆกลางเป็นสิ่งแพร่หลายในโลกของธุรกิจ โดยการบริการแบบกลุ่มเมฆช่วยให้องค์กรลดต้นทุนคงที่ของเทคโนโลยีสารสนเทศ และขนาดของการดำเนินธุรกิจ นอกจากนี้บริการดังกล่าวยังสนับสนุนให้องค์กรสามารถเข้าถึงข้อมูลสารสนเทสได้อย่างง่ายดายและเข้าถึงได้ทั่วโลก รวมถึงทำให้องค์กรมีความได้เปรียบในการแข่งขันเหนือคู่แข่งอื่นที่ไม่ใช้เทคโนโลยีดังกล่าว อย่างไรก็ตาม แม้ว่าการบริการแบบกลุ่มเมฆสามารถก่อให้เกิดประโยชน์แก่องค์กร แต่บริการนี้ก็เพิ่มความเสี่ยงด้วยเช่นกัน บทความนี้นำเสนอภาพรวมของการประมวลผลแบบกลุ่มเมฆ ในเรื่องของประโยชน์และข้อจำกัด รวมถึงวิธีการที่ตรวจสอบเทคโนโลยีดังกล่าว

คำสำคัญ: การประมวลผลแบบกลุ่มเมฆ การให้บริการแบบกลุ่มเมฆ การตรวจสอบ

Introduction

In the past decade the growth in use of information technology (IT) systems to support business processes has increased significantly. An average of 50 percent of an organization's capital expenditure budget is allocated to IT investment (U.S. Department of Commerce 2008). With this level of investment, corporations expect efficiency improvements, such as increased employee productivity and inventory management savings; other expectations include gains in effectiveness, such as improved customer relationships and management reporting quality.

Hoping to realize benefits of IT systems, but understanding that their core competency may not be technology, companies have been looking toward newer generations of cloud systems. This allows many companies to reduce the complexity and costs associated with traditional IT approaches, while enhancing internal efficiencies, expand flexibility, and increase scalability. Companies also should realize that although cloud computing systems provide huge advantages for businesses, they introduce additional risk concerns. Alali and Yeh (2012) reveal that companies adopting cloud computing systems are more likely to have material control weaknesses and may need to restate financial statements after adoption. The objective of this paper is to provide an overview of cloud computing as well as benefits and risks associated with cloud computing technology. Additionally, it points out how to effectively audit cloud computing.

Overview of Cloud Computing

Cloud computing is a new buzzword—but what does it actually mean? A cloud computing system is a pay-per-use consumption and delivery model that enables real-time delivery of configurable computing resources—for example, networks, servers, storage, applications, and services. These resources are usually delivered over the Internet to enrolled companies, who pay only for what they use (IBM 2012). Chou (2015) defines cloud computing as "a newly developed computing technology that utilizes virtualization resources to deliver IT services through the on-demand mode and Internet technology." Marston et al. (2011) defines cloud computing as "an information technology service model where computing services (both hardware and software) are delivered on demand to customers over a network in a self-service fashion, independent of device and location."

There are many cloud computing definitions. The National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce, provides standardized terminology. NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing comprises five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. NIST also identifies three cloud service models and four deployment models. The service models are:

- Software as a Service (SaaS). The capability provided to a consumer to use the provider's applications (and services) running on a cloud infrastructure.
- Platform as a Service (PaaS). The capability provided to a consumer to deploy onto the cloud infrastructure consumer-created or acquired applications developed using programming languages and tools.
- Infrastructure as a Service (IaaS). The capability provided to a consumer to access processing, storage, networks, and other fundamental computing resources, and the consumer is able to deploy and run software, which can include operating systems and applications.

The deployment models are:

- Private cloud, which is operated solely for an organization. It may be managed by the organization or a third party and can exist on or off the premises of the organization.
- Community cloud, which is a cloud that is shared by several organizations and supports a specific community that has a shared mission or interest. It can be managed by the community or a third party and can reside on or off the premises of the community.
- Public cloud, which is made available to the general public or a large industry group. It is owned by an organization selling cloud services.
- Hybrid cloud, which is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound by standardization that enables data and application portability.

Benefits and Points of Concern

Cloud computing provides several benefits. The major advantage is the reduction in capital investment, as companies can decrease the cost of IT infrastructure acquisition (Shimba 2010). Additionally, it allows companies to focus more on their business activities and leaves information systems to be taken care of by a cloud service provider. Cloud systems allow companies to access many customers with low cost (Neumann 2014), and to deploy new systems for new business services more rapidly with minimal cost (Protiviti 2012). The necessary resources can be acquired within a short period of time. Furthermore, cloud users can avoid traditional problems with respect to the waste and overuse of IT resources because the cloud providers allow flexibility in resource deployment in the users' operations (Armbrust et al. 2010).

Cloud computing not only provides benefits to enterprises but also introduces new risks to companies. Akande et. al (2013) present that cloud computing may raise many information system management issues. Examples of areas of concern include security, legal and jurisdictional, lack of standardized service level agreements, customizations, technological bottlenecks, strategy issues, change management, and disaster recovery. Ali et al. (2015) specify issues around data and storage, identity and access management control, web application and application programming interface security, service level agreement, and legal concerns.

These issues should be taken into account when companies consider using cloud computing services. As a result, security, legal, and service level agreements are three major concerns when enrolling in or developing cloud computing systems.

The security issues involve confidentiality, integrity, and availability. Confidentiality means that only an authorized person can access data. However, in cloud computing environments—since the resources such as networks, data, applications, and memory are shared among other users—there could be an increase in the risk of data compromise (Zissis & Lekka 2012).

Second is integrity. Integrity means only an authorized person can make changes to data, software, and/or hardware (Zissis & Lekka 2012). Authorization is a mechanism used to ensure that only necessary and appropriate permissions are given to a user to gain access rights to read, modify, or delete data. A cloud computing provider is required to maintain data integrity.

Third is availability. Availability is defined as data, software, and hardware which are accessible and usable on demand (Zissis & Lekka 2012). The system should continue working without interruption if a security breach occurs. Cloud computing providers should guarantee availability. However, one of the larger availability risks for cloud computing is the reliance of a wide area network, which generally requires the Internet or a private network spanning geographically disparate sites. If this connectivity is broken, services are disrupted across the entire network. Consequently, data in the cloud may be more vulnerable to risk in terms of confidentiality, integrity, and availability when compared to a conventional computing model.

A service level agreement is a document that identifies the terms and conditions between the user and cloud computing provider. The service level agreement may indicate guarantees of performance level, consequences in case of breach of the agreement between the user and cloud computing provider, billing, penalties, security, infrastructure, applications, etc. Therefore, companies or users are required to clearly understand the terms of the service level agreement, and all of the requirements in the service level agreement should be completely agreed upon (Ali et al. 2015, Neumann 2014, Akande et al. 2013).

Legal issues also arise for cloud computing because the data center may be located in country other than the users', and these countries may have different laws or regulations related to the service agreement. It also may be difficult to configure the security policies to comply with any newly promulgated laws. It is possible that data may be presented in more than one location that has different laws on information security. Thus, when the data of a particular cloud user is seized due to an investigation, it is possible that other users' information in the same cloud system also can be breached (Ali et al. 2015, Neumann 2014, Akande et al. 2013).

In sum, cloud computing provides huge advantages to companies but also introduces elements of risk. Before adopting cloud services, management should consider thoroughly both pros and cons, and negotiate contracts appropriately.

Auditing Cloud Systems

Cloud computing is classified as a special case of outsourced IT operations by the American Institute of Certified Public Accountants (AICPA). Although companies transfer out IT services to cloud providers, it does not transfer out the accountability of those services to the cloud service provider. Auditors who audit cloud users need assurances about the controls at cloud service providers.

At the Institute of Internal Auditors (IIA) Chicago Chapter 53rd Annual Seminar in 2015, Mr. Phillip Lageschulte, a partner of KPMG, provided five areas that auditors should consider when auditing cloud computing services. The five areas are identity and access management, data protection, technology risks, operations, and regulatory.

When auditing cloud systems, auditors should verify that only authorized people, based on their organizational roles, have access to the services and that this access is removed in a timely manner when that access is no longer necessary. Policies and procedures to protect data should be proven implemented and operating effectively. In addition, auditors should ensure that integration methods used by cloud service providers are standardized and can be imported or exported in standard formats. Moreover, auditors should assess procedures related to incident management, problem management, as well as change and access management in the context of usage of cloud services. Finally, the protection of information should be compliant with all relevant regulatory requirements.

Conclusions

According to an IBM survey, by 2020 the global cloud computing market will have grown 22 percent annually to US$241billion. Almost three-quarters of the survey participants indicate that their companies have piloted or adopted cloud usage. Cloud computing not only changes the way organizations manage IT systems, but also bring new challenges to the organizations and to auditors as well.

Organizations should evaluate the advantages and disadvantages of cloud computing before adoption. The controls over cloud computing should be implemented. Auditors should be familiar with this technology so as to assess IT risk level accurately; if the IT risk is high, the risk of material financial misstatements increases as well (Grant et al., 2009). An under or over estimation of IT risk level can lead to inappropriate audit planning and underperforming audit execution.

References

Alali, F. A. & Yeh, Chia-Lun. (2012). Cloud computing: Overview and risk analysis. *Journal of Information Systems, 26* (2), 13–33.

Ali, M., Khan, S.U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357–383.

Akande, A. O., April, N. A., & Van Belle, J. (2013). Management issues with cloud computing. ICCC'13, December 1–2, 2013, Wuhan, China.

Ames, B. & Brown, F. (2011). Auditing the cloud. *Internal Auditor*, August 2011, 35–39.

Armburst, M., Fox, A., Griffith, R., Joseph A., Katz R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. (2010). A view of cloud computing. Communication of the ACM, 53 (4), 50–58.

Chou D. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces. 42*, 137–142.

Grant, G. H., Miller, K. C., & Alali, F. (2009). The effect of IT controls on financial reporting. *Managerial Auditing Journal, 23* (8), 803–825.

Howell, J. (2015). Moving to the cloud. *Strategic Finance*, June 2015, 31–35.

IBM. (2012). The power of cloud driving business model innovation.

KPMG. (2013). Cloud computing risks and auditing. IIA Chicago Chapter 53rd Annual Seminar.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—the business perspective. *Decision Support Systems, 51*, 176–189.

National Institute of Standards and Technology (NIST). (2011). The NIST definition of cloud computing.

Neumann, P. G. (2014). Risks and myths of cloud computing and cloud storage. *Communications of the ACM, 57* (10), 25–27.

Protiviti (2011). Internal audit's role in cloud computing.

Shimba, Faith. (2010). Cloud Computing: Strategies for Cloud Computing Adoption. Lambert Academic Publishers.

U.S. Department of Commerce. (2008). The Statistical Abstract: Information and Communication. Suitland, MD: U.S. Census Bureau.

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28* (1), 583–592.