屏科大 National Pingtung University of Science and Technology

Governance Model of Cloud Computing Service

Wen-Hsi Lydia Hsu

Associate Professor, Department of Business Administration, National Pingtung University of Science and Technology
hsuw@mail.npust.edu.tw 886-8-770-3202#7698

Abstract

Cloud computing adoption by organizations has been surged with rapid growth. The major concerns stem from cloud computing services are security risk, loss of control and inadequate risk management.

This paper provides a conceptual framework of cloud computing governance from the perspective of education and proposes a four-stage procedure to establish a cloud computing governance model. The model provides useful insights into how enterprises govern their cloud computing and related risks. With the increased importance of continuing learning and education, the model also integrates education and learning into the model.

An adequate cloud computing governance model will help organizations to ensure a secured cloud computing environment and to comply with all relevant organizational information technology policies and ultimately will enhance corporate performance.

The proposed model may contribute to the cloud computing practices by providing guidelines to management on how to implement cloud computing governance framework. It will not only benefit to the sector of cloud computing but also to the sector of education.

Index Terms-Cloud Computing, Education, Governance, Security Risk

I. Introduction

CLOUD computing refers to an on-demand service delivery model that normally spans both outsourced and premises-based platforms [4]. According to a survey based on responses from 2,014 Chief Information Officers (CIOs) in 50 countries, 3% of CIOs report that they have the majority of information technology (IT) running in the cloud in their companies in 2011. Nevertheless, 43% of companies projected that their IT efforts will be running in the cloud in 2015. With the rapid growth of cloud computing, it has emerged as an important platform, offering enterprises a potentially less expensive model to deal with their daily computing needs and accomplish business objectives [2].

Cloud computing provides corporations with many potential benefits. However, there are also many information security risks in cloud computing environment that affect the corporate strategy. As cloud computing continues to grow, the need for a governance strategy and a good governance model will become more important. Effective governance of cloud computing can be of benefit to enterprises, including senior management, audit committee and board of directors.

According to the book recently released by the global IT association ISACA entitled "IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud ", it indicates that, in order to get the most benefit from cloud computing initiatives, companies need to develop a clear governance strategy and management plan that sets the direction and objectives for cloud computing [9] [2].

Consequently, this study attempts to develop a governance model to provide insights into how enterprises govern their cloud computing applications and related risks and the important role of continuing education in the process of implementation. More specifically, the objective is to provide an understanding of cloud computing and identify the related risks and controls to build effective governance mechanisms and frameworks. The education of cloud computing knowledge and ongoing learning in the process of governance are important factors that facilitate an effective and successful governance model. The results may provide useful guidance for companies that are considering promoting data and business processes into a cloud environment and to the education and practice as how to implement an effective governance for cloud computing.

This study contributes to the existing literature towards building a theoretical base for the key issues and factors of effective cloud computing governance model during implementation processes. Furthermore, it also provides guidelines to executive managers about cloud computing governance framework implementation. It will not only benefit to the sector of cloud computing but also to the sector of education.

The remainder of this paper is organized as follows. The second section outlines the characteristics of cloud computing and its benefits and risks. In the third section, it proposes a cloud computing governance model with an emphasis on the continuing education and learning in the process of implementation. The final section ends with a conclusion.

[1] *ISACA (www.isaca.org), previously known as Information Systems Audit and Control Association, is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance.*

II. An Overview of Cloud Computing

Cloud computing is defined by the US National Institute of Standards and Technology (NIST) 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[8] (p.2)" .Cloud computing technologies can be implemented in a wide variety of architectures under different delivery service and deployment models. The cloud model is composed of three service models and four deployment models as discussed below.

A.Cloud Computing Service Models

Cloud service can be categorized into three delivery models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [2][3][8]as illustrated in Fig. 1. Each model delivers different computing service to the customer. SaaS offers customers to use the applications running on a cloud infrastructure constructed by a cloud service provider (CSP). The services are accessible from various client devices, such as a web browser (e.g., web-based email) or a program interface. Examples of popular consumer-directed SaaS applications are Facebook, G-mail™, Yahoo® user applications, Google Docs and Microsoft® Online Services. Consumers do not need to manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [2]. PaaS provides customers to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The PaaS provider offers customers elemental service-oriented architecture application building blocks to configure a new business application. PaaS users have control over the deployed applications and possibly configuration settings for the application-hosting environment. Examples of PaaS providers are Microsofts Azure™ Service Platform, Googles Google App Engine [2][8]. IaaS offers the consumer to provision processing, storage, networks, and other fundamental computing resources, allowing the consumer to deploy and run arbitrary software, which can include operating systems and applications [8]. IaaS provides online processing or data storage capacity. It is suitable for the enterprises with very large data storage, one-time processing demands [2][3]. Amazon Web Services™ is one of the examples of IaaS service provider [2]. Each of the above mentioned cloud service model has a different level of business risk. Companies need to establish their own governance models to ensure that cloud computing services are well defined and operated in a secure environment within its existing information technology (IT) operations.

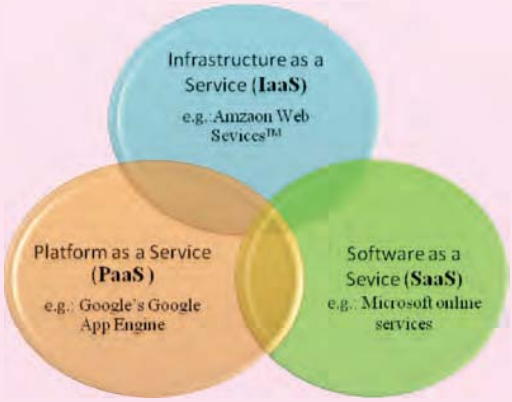

Fig. 1 Cloud Computing Service Models (Mell and Grance, 2011)

B.Cloud Computing Deployment Models

The three above mentioned cloud service delivery models are offered to cloud customers in four cloud deployment models: private, public, community and hybrid, as illustrated in Fig. 2.

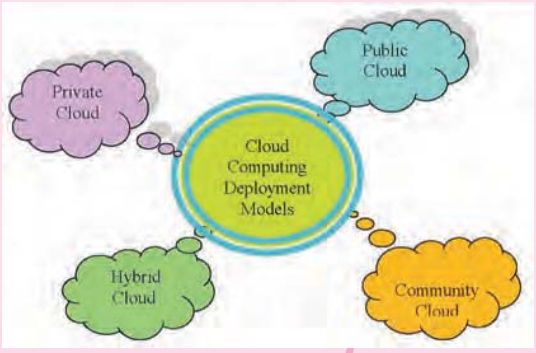

Fig. 2 Cloud Computing Deployment Models

Deployment models broadly characterize the management of disposition of computational resources for delivery of services to consumers, as well as the differentiation between classes of consumers [3]. A Public cloud is one in which the infrastructure and computational resources that are made available to the general public [1]. A private cloud is one in which the computing environment is operated exclusively for a single organization. A community cloud falls between public and private clouds with respect to the target set of consumers [8]. The infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security and regulatory considerations for a shared purpose [3]. A hybrid cloud is more complex than the other deployment models as they involve a composition of two or more deployment models at the same time allowing for data and application sharing [1][3][8].

III. Governance Model of Cloud Computing Service

With the collapse of Enron, corporate governance has attracted much attention worldwide and has taken center-stage across boardrooms around the world. Given the fact that cloud computing is expected to play a key role in helping organizations achieve their business objectives, it is essential to address the role of corporate governance over cloud computing. The responsibilities of board of directors are discussed first, followed by a proposed four-step procedure to establish a cloud computing governance model with the emphasis of continuing learning and education in the process of governance.

A.Director Responsibilities for Cloud Computing Governance

Recent studies on corporate governance has raised the level of interest in directors' responsibilities on IT governance [11]. Information Technology (IT) and the emerging technology of cloud computing were two major monitoring concerns identified by the members of audit committee in a conference held in 2011[6]. Although cloud computing was recognized as an important issue for companies, a survey by Portio Research revealed that more than 50% of IT decision-makers reportedly know very little about cloud computing [12]. The lack of understanding of cloud computing raises questions of governance and may put enterprises in danger of losing competitive advantage.

Cloud service presents the opportunity and will add value to the organization if it is fully align with the goals of the enterprise as a whole. The adoption of cloud computing impacts business processes, making governance critical to control risks effectively [9]. The general responsibilities of board of directors in an organization are to supervise the management and the operation of business [11]. The monitoring function of boards in organizations is one of the important governance mechanisms. Board of directors need to evaluate their existing governance against security risks associated with cloud computing services and the impact on corporate strategy. Organizations must be well prepared in implementing necessary compensating controls over cloud computing.

Typically, the responsibilities of directors with regard to internal control are delegated to the audit committee, which places a considerable emphasis on the appropriateness of internal and external auditors and their review with regard to control issues [11]. The audit committee in an organization should require that any selected cloud computing solution is configured, deployed and managed to meet their organizational security, privacy and other requirements. Governance issues for concern may include risk management, disaster recovery plan, vulnerability assessment, business continuity, incident response, encryption identity, access management and virtualization [5]. Directors need to determine that the management is taking the steps necessary to ensure a good system of governance is in place.

B.Procedure in Implementing Cloud Computing Governance Model

In order to establish an effective cloud computing governance model, the study proposes a four-stage procedure as illustrated in Fig. 3:

Stage 1: Set Up Cloud Computing Policies and Standards

Good Standards and practices will assist cloud governance to establish cloud business objectives and risk considerations. Therefore, it is important that companies establish their cloud computing standards and policies at the very first stage. The whole procedure is a continuing process and is performed based on the framework of cloud computing standards and policies.

With IT budgets increasingly allocating money for cloud services and the growth in cloud adoption, ISACA [2] points out that it is important for organizations to wrap their arms around the benefits of this technology and the role of governance. To get the most benefit from cloud initiatives, enterprises must develop a clear governance strategy and management plan that sets the direction and objectives for cloud computing [2]. Accordingly, Information security risk management is a critical component of cloud computing governance [1]. Risk management helps organizations recognize the wide spectrum of cloud computing risks that they are exposed to and prioritize cloud computing risks based on their potential impact.

Stage 2：Evaluate Risks Associated with Cloud Computing

To establish appropriate governance mechanisms of cloud computing, the audit committee should set up cloud computing policies to assess the risks and opportunities cloud computing presents to their companies. This raises a question as to whether directors on boards have the expertise to evaluate whether the procedure of assessment in place is appropriate or effective. In order to examine if the organizations meet their cloud computing policies and criteria and to help directors fulfilling their IT responsibilities, ISACA suggested organizations to ask the following questions [2] before applying cloud computing services:

- What level of availability does the organization expect from the cloud service?
- How are identity and access managed in the cloud?
- Where will the organization's data be located?
- What are the service provider's disaster recovery capabilities?
- How is the security of the organization's data managed?
- How is the whole system protected from Internet threats?
- How are activities monitored and audited?
- What type of certification or assurances can the enterprise expect from the provider?

As the security issue is one of the key factors for corporate strategy about outsourcing information technology services to a cloud computing environment, board of directors in enterprises should follow the governance model in analyzing available security and privacy options to place companies' functions to a cloud environment. Boards need to understand the immediate risks of cloud computing and to openly embrace and advance the risks that cloud computing presents.

Stage 3 ：Involve Management in the Process of Cloud Computing Governance Model

To establish appropriate governance of cloud computing, The Chief Information Officer (CIO) plays a significant role in supporting boards, audit committees and the management to understand and implement good governance over cloud computing [7]. CIOs need to exercise their responsibilities of due diligence to ensure that all the criteria are met. After implementing cloud computing service, enterprises need to evaluate their vulnerabilities, threat prevention policies and technologies periodically and feedback to their directors on board who are responsible for IT governance.

Stage 4 ：Evaluate Performance

It is important to evaluate the performance of cloud computing governance model to align with its strategic priorities. A well-designed cloud computing governance model ensures that these policies and standards are consistent with the strategy of the organization. Business Intelligence (BI) can also be applied to design the performance measures to monitor the effectiveness of cloud computing governance. Both performance dashboards and balanced scorecards (BSC) can be instrumental in helping organizations communicate their strategic objectives to meet their goals or their key performance indicators (KPIs).

C.Education and Learning in Governance Model

(1)On-going Learning and Education throughout the Whole Organization

During the process of implementing the governance model, education is one of the factors that lead to an effective governance. As Tillery [10] emphasized, the greatest IT security threat stems not from the cloud itself, but from having inadequate IT security policies and a lack of education about employees' role in defending a company's data. Consequently, educating employees about cloud computing related risks and governance processes is important and should start from bottom to top with an ongoing learning process across the organization. It is the responsibility that rests on the management to extend this governance model into the rest of the whole organization by educating employees the policies and standards with regard to cloud computing practices.

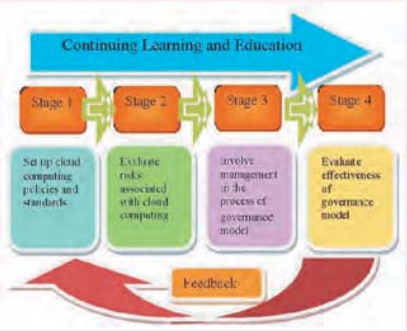

Fig. 3 A Four-stage Procedure of Cloud Computing Governance Model.

IV. Conclusion

Cloud computing technologies can be utilized in a wide variety of architectures, with a form of different delivery service deployment models. The security risks challenges cloud computing are dreadful, including those faced by public clouds whose infrastructure and computational resources are owned and operated by an outside party that delivers services to the general public via a multi-tenant platform. Far from being a threat, the popularity of cloud computing offers new opportunities to businesses. Accordingly, there is a need to develop a cloud computing governance model.

The study proposes a four-step procedure to establish a cloud computing governance model. As cloud computing continues to increase its importance to business daily operations, it is essential that enterprises understand how to best handle the paradigm change that the cloud presents. This level of understanding will enable enterprises to maximize the benefits that cloud platforms offer, while simultaneously become less vulnerable to security risks.

Over the next few years, companies will create and transmit more data than was previously created and transmitted. Cloud computing will be great of significance in helping meet the demands. Given the importance of cloud service strategies and the related risks on business operation, directors on boards need to understand and monitor their company's cloud strategy. Before involved in cloud computing service, it is essential to have the necessary education of cloud computing knowledge, IT expertise and governance processes to manage the use of cloud computing. Continuous learning is one of the successful factors in implementing a cloud computing governance model. Companies that understand the impacts of cloud computing and that can acquire skills necessary to set the proper security policies will be able to mitigate the risks associate with cloud security.

Enterprises should carefully plan the security solutions and educational schemes before engaging in cloud computing service. The governance model in the study may provide a helpful tool for education and practice.

References

[1]R. Farrell, 2010, "Securing the cloud-governance, risk and compliance issues reign supreme," Information Security Journal: A Global Perspective, 19, pp. 310 – 319.

[2]ISACA (Information Systems Audit and Control Association), 2011, IT control objectives for cloud computing: controls and assurance in the cloud, ISACA. [3]W. Jansen, and T. Grance, 2011, Guidelines on security and privacy in public cloud computing, National Institute of Standards and Technology (NIST), Department of Commerce, USA. NIST Special Publication 800-144 (http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494).

[4]J. Kobielus, 2009, "Storm clouds ahead: SOA governance clashes with cloud computing model," Network World, 26(9), pp. 24 – 28.

[5]J. Leonard, 2011, "Changes in governance, security," Network World, 10/10/2011, 28 (18), p.28.

[6]M. P. McCarthy and S. Hill, 2011, "Cloud adoption points to IT risk and data governance challenges," NACD Directorship, April/May, p. 72.

[7]C. R. McClure and J.C. Bertot, 2000, "The Chief Information Officer (CIO): Assessing its impact," Government Information Quarterly, 17(1), pp. 7-12.

[8]P. Mell and T. Grance, 2011, The NIST definition of cloud computing, Special Publication 800-145, National Institute of Standards and Technology, September, <URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf >.

[9]S. Steffee, 2011, "Cloud computing governance remains elusive," Internal Auditor, 68(5), p.14.

[10]S. Tillery, 2010, "How safe is the cloud?" Baseline, September/October, p.15.

[11]G. Trites, 2004, "Director responsibility for IT governance," International Journal of Accounting Information Systems, 5, pp. 89-99.

[12]P. Williams, 2009, "Governance in the cloud: head in the sand? Computer Weekly, 12/8.