Computer Standards & Interfaces 42 (2015) 137–142

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Cloud computing risk and audit issues

David C. Chou *

Department of Computer Information Systems, Eastern Michigan University, Ypsilanti, MI 48197, USA

ARTICLE INFO

Article history:
Received 6 September 2014
Received in revised form 27 May 2015
Accepted 16 June 2015
Available online 20 June 2015

Keywords:
Cloud computing
Auditing
Risk factors
Audit standards

ABSTRACT

Cloud computing has gained mass popularity in the business environment. However, this technology also imposes some risk concerns, such as weak protection to security and privacy. Since its nature of distant and remote connectivity, the auditing process to this technology becomes challengeable. This paper focuses on issues related to cloud computing risk and audit tasks.

1. Introduction

Enron and WorldCom financial scandals raised concerns by government about accounting errors and fraudulent practices created within organizations. The Sarbanes–Oxley Act (SOX) of 2002 was legislated to require CEOs and CFOs in publicly traded U.S. organizations to personally certify and be responsible for their company's financial statements. Since SOX commands the storage times for specific financial records, it thus requires IT departments to maintain such electronic records. SOX stipulate that all business records and e-messages must be saved for not less than five years. For this reason, organizations using IT for financial processes must conduct IT controls to comply with SOX legislation. IT auditing thus becomes a mainstream in auditing practices.

The coverage of IT auditing is broad since public organizations adopt information technology for processing their business data. No matter what business models (either regular business or electronic business) they adopt, all financial data and messages would be handled by ICT (information and communication technology) systems. In order to pursue SOX compliance, a secured and risk-free IT control is mandated. Therefore, a complete IT auditing should examine a company's internal information systems and their inputs, outputs, and processing components. Other supplementary examination should include IT department's hardware, software, communication networks, interfaces, etc. Another goal of IT auditing is to identify and monitor various risks that may reside in the IT operational processes.

A newly developed computing area—cloud computing—has been adopted by a number of organizations for various purposes. Organizations move to cloud computing practice may gain possible benefits such as cost saving, efficiency improving, agility enhancing, flexibility and scalability expansions, and environmental sustainability. Cloud computing is gaining popularity since it changes the IT industry by sharing resources through the idea of virtualization. In the meantime, one major concern to cloud computing is its virtualized environment. The operation of cloud computing is similar to the practice of information systems outsourcing. The similarity between the two is the use of external vendor's hardware, software, infrastructure, or storage capabilities for internal ICT processes.

The purpose of this paper is to discover the challenges faced by cloud computing audit. Since cloud computing may become the next wave of IT innovation, organizations may adopt this technology for major business processes. Therefore, a clear examination of cloud computing audits may contribute to the field by providing auditors a vibrant practical guidance. The structure of this paper is as follows: the next section discusses the rise of cloud computing. It then provides a detailed discussion to IT auditing and some IT auditing methods in the next two sections. After that, the process of cloud computing auditing is discussed. Guidelines about cloud computing audit then follow. The next section points out standards, challenges, and future of cloud computing auditing. A conclusion to this paper is presented in the last section.

2. The rise of cloud computing

The rise of cloud computing is closely related to the increasing practice of information systems outsourcing. We first discuss the implication of information systems outsourcing. Information systems outsourcing is an important practice in business operation, which hires outside IT professional services to meet a company's in-house needs. Business process outsourcing (BPO) has been integrated into

* Corresponding author. Tel.: +1 734 487 0054.
E-mail address: dchou@emich.edu.

http://dx.doi.org/10.1016/j.csi.2015.06.005
0920-5489/

corporate management as an organizational strategy [2]. Although IS outsourcing practice gains a number of benefits such as reducing operational cost, accessing new and updated technologies and capabilities, sharing resourcing and risk, etc., there are risks involved in such a process. Information systems outsourcing risks affect the service quality to customers directly and indirectly. Areas of information systems outsourcing risks have been reported in switching costs [24], unexpected transition and management costs [8], disputes and litigation [19], costly contractual amendments [10], service debasement [19], loss of organizational competence [10], cost escalation [19], and hidden service costs [19]. Since information systems outsourcing projects involve external organizations for software construction and maintenance, the probability of risk occurrences are relatively higher than that of in-house projects.

The theoretical foundation of information systems outsourcing has been discussed by [2]. Chou [2] identified several theoretical sources, including transaction cost theory [29], production cost economics [30], competitive advantage and value chain [31], resource based theory [32], and economies of scale [2].

Chou and Chou [4] proposed an information systems outsourcing life cycle model and its risk analysis. The concept of information systems outsourcing life cycle describes "a sequence of activities to be performed during corporate IS outsourcing practice [4, p. 1038]". Based on their model, the whole IS outsourcing life cycle consists of three phases and seven activities. The pre-contract phase contains activities such as identifying the need for outsourcing, planning and strategic setting, and outsourcing vendor selection. The next phase, contract phase, has to do contracting process, transitioning process, and outsourcing project execution. The last phase, post-contract phase, performs outsourcing project assessment activity [4, p. 1038].

Each phase and activity in information system outsourcing life cycle may encounter risks and uncertainties. For example, the pre-contract phase may run into the risk of outsourcing planning deviations such as lack of market and vendor's information. During the contract period, many technical and managerial risks may be appended. Even the post-contract period may face risks such as the lack of assessment measurement and quality model. In order to identify the risks factors and monitor the quality of IS outsourcing practice, a rigid auditing practice should be applied to the whole outsourcing life cycle.

Cloud computing is a newly developed computing technology that utilizes virtualization resources to deliver IT services through on-demand mode and the Internet technology [6]. [33, p. 177] defined 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." The operational model of information systems outsourcing is closely comparable to that of cloud computing's, both practices demonstrated the capability of resource utilization, virtualization, scalability, and agility.

The National Institute of Standards and Technology (NIST) also defined cloud computing as "a model for enabling 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." [22]. Based on the NIST's classification, private cloud, community cloud, public cloud, and hybrid cloud are the four major patterns of cloud deployment [22].

A private cloud is operated solely for an organization that does not share hardware or infrastructure with other companies. Mell and Grance [21, p. 3] described a private cloud as "the infrastructure provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises." A private cloud provides internal services to its organization through company-controlled intranet or data center. This cloud service can offer needed fault tolerance and security that company requested [6].

A community cloud is formed by the shared concerns, such as mission, security requirements, policy, and compliance consideration [21]. A community cloud can be created and operated by individual or multiple organizations in the community, located inside or outside the organization.

A public cloud has been adopted by most organizations for cloud computing practices. A public cloud's service providers (Google or Amazon.com are examples) offer their cloud infrastructures for any organization's usage, on a self-service, on-demand, and pay-per-use basis. The infrastructure of a public cloud exists inside the cloud provider [6].

A hybrid cloud is the last type of cloud service. The cloud service combines a variety of cloud infrastructures to fulfill its specific need. It is a mixture of public cloud, private cloud, and community cloud options. An organization may consider its strategic needs and/or security concerns to distribute work capacities into separate cloud infrastructures [6].

These cloud deployment patterns reflect the cloud computing's operational differences in areas of location selection, infrastructure placement, resource sharing option, and openness of provision. The variance in cloud computing's deployment may cause operational difference in auditing practice. Issues in cloud computing audit will be discussed in later sections.

Cloud computing contains three types of service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [22]. SaaS is a popular cloud service that allows consumers to use provider's applications/software that can be accessed through a program interface or a web browser. The consumer does not need to install IT infrastructure such as network, servers, operating systems, and application software inside individual company but to be hosted and managed in the vendor's site. PaaS is a cloud service model that provides corporate IT's need by housing the entire computing platform (such as networks, servers, operation systems, or storage) and solutions that are needed at the client's site. However, PaaS service model allows the client to control the application software and interface programs [6]. IaaS is a cloud service model that "offers clients the capabilities of processing, storage, networks, and other computing resources so they can run selective software (operating systems and applications) in-house. The only tradeoff is that cloud providers manage the infrastructure in use" [6, p. 73].

Similar to IS outsourcing practice, cloud computing clients (or user companies) acquire their needed infrastructure, platform, data storage, and/or software programs from cloud service providers (or vendors) for receiving on-demand and pay-per-use service. Most cloud providers offer metered service—it means they charge customers only for the processing capacity that customers actually used. Both IS outsourcing and cloud computing practices utilize external information systems resources to gain the advantages of economies of scale and value creation. Therefore, IS outsourcing and cloud computing perform similar information processing models, it makes their auditing work different from that of traditional information systems. We will discuss this issue in detail in the next section.

3. IT auditing: Concepts and techniques

The exercise of auditing is required by law. The main implication of auditing is "an independent examination of an organization's management assertions that must follow a set of guidelines and standards promulgated by an external sanctioning body" [20]. The audit examiner, or auditor, could be an internal auditor or external auditor from CPA firms. The audit area may be varied; however, the primary auditing area should be accounting and financial sectors in an organization. IT auditing either covers specific focus (such as database, network, system development, security, application systems such as enterprise resources