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/© 2015 Elsevier B.V. All rights reserved.

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 planning (ERP) and customer relationship management (CRM), IT governance, and cloud computing) or examines information system controls in inputs, outputs, and processing in an organization.

IT auditing offers an important service to organizations that offer computing capability to deliver internal and external business processes. The main purpose of IT auditing is to examine whether an organization's information systems operation and management follow a set of guidelines and standards disseminated by an external standardization body. The structure of an IT audit is a logical process that contains three phases: audit planning, tests of controls, and substantive testing [15]. The first phase, audit planning, is necessary because the auditor must well prepare the auditing work before everything starts. Information must be collected and analyzed by the auditor, such as client's business and IT processes, internal controls, and their potential risks. The ways of conducting planning work can go through documentation review, questionnaires filling, employee interviews, and possible work observation. The second phase, tests of controls, investigates the adequacy and functionality of various internal controls over IT activities. During this phase, the auditor must perform control tests over IT activities and collect evidence on control quality and control risk at client side. The third phase, substantive testing, centers on the financial side of the IT operation. Data such as specific account balances and transactions should be examined carefully to ensure the full quality of the enterprise database [15].

The audit planning phase contains three stages, including (1) reviewing the organization's policies, practices, and structure; (2) reviewing the general controls and application controls; and (3) planning tests of controls and substantive testing procedures. The tests of controls phase consists of the following stages: (1) performing tests of controls, (2) evaluating test results, and (3) determining the degree of reliance of the controls. The substantive testing phase has the following stages: (1) performing substantive tests, (2) evaluating the results and the issue auditor's report, and (3) generating an audit report [15].

The main purpose of an IT audit is to check the quality of IT operational processes within an organization. A quality audit is "defined by ISO as a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives" [5, p. 558]. It is clear that the concept of quality audits can be applied to all auditing areas, including IT auditing practice.

Merhout and Havelka [20] proposed an IT audit quality framework, in which eight components were identified as the constituent success factors of IT audit. Through this quality framework, we can clearly understand the major influence factors of IT auditing success. These components and factors are listed below.

- *Audit team factors*: team communications, experience working together, and cohesiveness
- *Audit process and methodology factors*: the existence of an audit methodology for the team to follow, scope of definition, the use of automated tools, and timely oversight/review of audit work
- *Client-controlled organizational factors*: management's support and adequacy of documentation; relationships with clients, adequate time allocated for the entire audit, leadership, and understanding of business unit and IT organization initiatives and changes
- *IT audit personnel technical competency factors*: understanding of risks and control weaknesses, project management, and staff experience
- *IT audit personnel social and interpersonal factors*: independence, communication skills, willingness and ability to change, and motivation/enthusiasm
- *Enterprise and organizational environment factors*: financial resources, corporate culture, the reporting structure of internal audit, perception of value added from audits, and the number of recent audits, and
- *Target process or system factors*: clearly defined project scope, system complexity and type, amount of manual versus automation in process, and the level of documentation for the process or system.

There are two specific IT auditing methods that have been recommended in the field, they are value-added audit and risk-based audit. These IT auditing methods are discussed in the next section.

4. IT auditing methods

Merhout and Havelka [20] indicated that IT audits can offer additional value beyond the objective of IT assurance. In general, the auditing process consists of four stages: preparation, performance, reporting, and closure [5]. Chou and Chou [3] applied this method to IT change management auditing processes. Although Chou and Chou's [5] auditing process focuses on the general auditing process, it fits well to IT auditing practices.

The purpose of IT auditing is to check whether or not the organization's IT processes meet its goals and objectives. Based on the variance of auditing goals, we can classify them into two major streams: value-added IT audit and risk-based IT audit. We will discuss the implications of these two IT audit methods. We start with the value-added IT audit method.

4.1. Value-added IT audit

Value-added audit is a new trend in IT auditing practice. Value is based on the quality of the business processes that meets various goals set by stakeholders, including customers, shareholders, employees, and government. A value-added audit intends to conduct the auditing work that monitors the organization's business processes (such as accounting, finance, quality, IT, etc.) for corporate value safeguarding and regulatory compliance. Specifically, a quality audit should cover the following areas: operational and quality effectiveness, business risks, business and/or process controls, process and business efficiencies, cost reduction opportunities, waste elimination opportunities, and corporate governance effectiveness [16].

Institute of Internal Auditors (IIA) [17] defined value-added auditing as "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes." Hutchins [16] further inferred this definition and then defined the value-added audit as "provide independent and/or objective operational analysis, to examine every function, process and activity of an organizational and external value chain, to help an organization achieve its business strategies and objectives, to follow a systematic and disciplined approach in its assessment, and to evaluate and improve the effectiveness of risk management, control and governance processes."

The benefits of value-added IT audit are widely covered. Merhout and Havelka [20] pointed out the following six benefits of exercising value-added IT audit: (1) improved return on investment in information technology through improved IT governance; (2) using audit documentation to improve operational efficiency through business (and IT) process reengineering or improved business process management; (3) using audit observations to improve risk mitigation through enhanced enterprise risk management (ERM) awareness; (4) improved business continuity planning and associated systems disaster recovery planning; (5) improved systems development quality; and (6) increased organizational communication and trust development through facilitation among various stakeholders.

Value-added IT audit is an extension of value-added audit process. The focus of value-added IT audit is on the organization's information and communication technology (ICT) operation and capability. Various values can be generated if the company passes the value-added IT auditing process. We will further discuss the new application of value-added cloud computing audit area in a later section.

4.2. Risk-based IT audit

Business risk audit (BRA) has gained wide attention in auditing firms [26]. A risk-based audit approach used to apply to internal audit practice. Fraser [11] described risk-based audit as "designed to be used throughout the audit to efficiently and effectively focus the nature, timing, and extent of audit procedures to those areas that have the most potential for causing material misstatement(s) in the financial report." This concept can be applied to IT auditing practice.

A risk-based IT audit is different from value-add audit due to their focal alterations. Since value-added IT audit targets value creation and quality maintenance of IT function, its purpose is to maximize the IT quality and capability in the organization. A risk-based IT audit, on the other hand, minimizes the risks that may be encountered by corporate IT operations. Specifically, risk-based IT audit identifies substantial IT threats and defines the audit tests and procedures for assessing internal controls over related IT functioning areas. A broader auditing area may include IT governance, systems security, systems development, and software change procedures.

5. Cloud computing auditing

More and more companies have recently adopted cloud computing services. Gartner Inc. forecasted that the sale for cloud services will increase from US$46.4 billion in 2008 to US$150.1 billion in 2013 [14]. The rise of cloud computing attracted IT auditor's attention, especially regarding the possible risks associated with such technologies. Under such circumstance, IT auditors must understand the details of cloud computing and follow a specific auditing method/approach that can comply with regulations set by auditing authorities for conducting auditing work. However, the values and risks of implementing cloud computing are the major focus in cloud computing auditing.

Since cloud computing involves outside vendor's support and control to desired information technologies, the auditing work should be more complicated than the regular IT auditing work [12,25,27,28]. Risk-based IT auditing is one of the important auditing methods that we discussed before. As long as IT auditors of cloud computing follow an auditing framework and select an effective risk assessment method, the cloud computing audit work would be similar to the work of regular IT audit.

The main risks of cloud computing technology are related to the following areas: authentication, data security and privacy, interfacing with internal systems, system availability, business continuity, and ownership of content and other legal requirements [25]. Among these risk factors, security and privacy are the most concerned areas since cloud computing data are stored outside corporate premises [23].

An alternate way of conducting cloud computing audit is through a value-added approach that we discussed earlier. The auditors should first clearly understand the cloud computing technology and the value that it could create after being adopted by the organization. The auditing work may then focus on those targeted value propositions. Possible values and benefits of adopting cloud computing are the following: solutions for every need and budget, increased flexibility, better resource utilization, improved efficiency and greater agility, access to new technology, improved security, cost avoidance, new cost model, and improved collaboration [7]. Value-added cloud computing tasks can be easy if the target value components can be identified and checked by an IT auditor.

An organization that adopts cloud computing services implies that it is outsourcing its IT functions to external vendors. Under SOX regulations, the client company cannot surrender its management responsibilities over internal IT control. The Auditing Standard No. 2 (stipulated by the Public Company Accounting Oversight Board) states that:

> "The use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting. Rather, user management should evaluate controls at the service organization, as well as related controls at the user company, when making its assessment about internal control over financial reporting."

The above standard stipulates that cloud computing adopters must conduct an evaluation of the vendor organization's IT control environment. The SAS 70 (Statement on Auditing Standard No. 70) auditor's report from the vendor's site should meet the goal of this stipulation, although this auditor's report is prepared by the vendor's auditor. Since there are two types of SAS 70 reports—type 1 and type 2 audit reports. Type 1 audit focuses on the fairness of the presentation of the service organization's controls. Type 2 audit focuses on whether specific controls were operating effectively. Since cloud computing technology is more complicated than regular outsourcing practice, conducting a type 2 audit may show more detailed controlling information from the vendor's site [9].

ISACA (Information Systems Audit and Control Association) has developed four new audit programs, these are cloud computing, crisis management, information security management, and windows active directory, to serve as the guidance for audit and assurance professionals [18]. Cloud computing programs cover "governance over cloud computing, the relationship between the service provider and customer, and specific control issues" [18]. This program provides a good tool and template for implementing cloud computing audit.

6. Guideline for cloud computing audits

As every IT auditor walks through a specific IT/IS organization, he/she will conduct an independent auditing process. Based on the circumstances of the audit task, such as the type of industry, size of the firm, and the IT infrastructure, the auditing activities would be unique and fit well. A cloud computing auditor may work in a specific cloud computing arrangement, such as private, public, community, or hybrid environment, with varied data storage arrangements and firm sizes, or within a specific industrial sector. For example, technological selection, information media, and data storage and its security are critical to financial and investment banks, healthcare institutions, and governmental agencies. On the other hand, logical attack, data integrity, and process speed are important for electronic business and mobile industries. Based on an organization's need, auditors must apply an appropriate audit approach.

According to ISACA [18], the cloud computing audit should cover the following three objectives:

- Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security
- Identify internal control deficiencies within the customer organization and its interface with the service provider
- Provide audit stakeholders with an assessment of the quality of and their ability to rely upon the service provider's attestations regarding internal controls

Although each cloud computing audit is unique, we can provide a general guideline for reference purposes. As indicated in the first section, cloud computing is similar to the practice of outsourcing of some combination of hardware, software, and data, which can then be accessed through Internet connectivity. While a firm intends to adopt cloud computing practice, the first important task is to select the right service provider. The next imperative work is to create a service contract with robust service level agreements (SLAs), in which all contractual obligations regarding security, assurance of information systems operations, and data storage should be clearly stated. In order to assure the service quality and to assess the risk of cloud computing environment, a firm must seek an audit request through internal or external auditors.

During the audit, the audit team should determine the focus of the auditing project. As indicated earlier, it may have value-added or risk-based audit processes. Either one should have a specific audit items to be checked. For example, value-added audit focuses on achieving improved return on cloud computing investment and risk mitigation. On the other hand, risk-based audit focuses on risk assessment, security, and data safety. The audit team then follows a specific standard or combined standards, frameworks, or guidance to check the compliance criteria. These standards are discussed in the next section.

The auditors need to create an audit report in which all checked items should be recorded. These audit items include all SLAs, governance, cost savings, data storage, risk and security issues, and disaster protection on cloud computing's operations within service provider and industry customer's sites. Basically, there are three sections that should be filled, these are relevant standard's objective, audit procedure, and findings. The relevant standard's objective section describes the individual audit standard's objectives that are to be audited for cloud computing compliance. The audit procedure section lists all audit steps and methodologies to be applied into such audit standard's objective. The findings section reports the auditing outcomes of each audit objective, including positive and negative observations and possible recommendations for improvement.

After the audit process, a firm should clearly understand the value of adopting a cloud computing environment. In the meantime, this firm should realize the strength and weakness of moving to cloud computing. Specific risk and security flaws and concerns can be revealed in the audit report. The firm's executives should find ways to resolve their IT weaknesses and then strengthen their overall business process management.

7. Standards, challenges, and future development

There are a variety of IT auditing standards that have been developed, such as COBIT (Control Objectives for Information and related Technology), COSO (Committee of Sponsoring Organizations) Enterprise Risk Management—Integrated Framework, ISACA's IT Assurance Framework, ITIL (Information Technology Infrastructure Library), ISO 27001, ISO reporting standard ISAE 3402, and SAS 70 [1,9,13,23,28]. Auditors may select one or combined standards for auditing practice. Most of these standards are applicable to IT auditing, which can be applied to cloud computing audit as well.

Several organizations such as US National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA), and European Network and Information Security Agency (ENISA) provide guidance and metrics to assess the risk and security of cloud computing implementation [13]. Their published documents can be utilized as a useful reference for cloud computing audits.

Cloud computing auditing is a complicated task in which various technological aspects need to be examined and reported. For example, organizations may adopt a public cloud, private cloud, community cloud, or hybrid cloud for their cloud computing practices. The complexity within these cloud categories may cost IT auditors tremendous amounts of energy to filter out the details of network connectivity, systems and software interfaces, database storage methods, platform differences, and infrastructure designs. Moreover, there are additional challenges to the new zone of cloud computing auditing that will be discussed in this section.

Security risk is the most significant concern to cloud computing technology. Since user organization's data are stored in a remote provider's area, it raises privacy and confidentiality concerns. Also, data transformation during cloud operation must pass through the Internet. Unless the providers offer absolute security programs to guard the data source and to prevent data breach during transmission, the trust relationship between vendor and client may not be easily established. Other than data security, there are plenty of risk components that need to be identified before IT auditors can start their work. Therefore, a well prepared work is essential to cloud computing's audit process.

Since cloud computing is a relatively new computing technology, technological weaknesses and immaturities may exist. In order to conduct a complete auditing process, these technological drawbacks need to be discovered and published. Therefore, this allows IT auditors to find the right area to examine the cloud computing process. This approach allows cloud computing's audit effectiveness to be achieved rapidly.

A non-technical challenge in cloud computing is related to contractual issues, that is, service level agreement (SLA) disputes between client and vendor. Since clients depend heavily on vendor's technology to run business and process data, a fully agreeable contract (including SLA) must be created and signed. Namely, SLA must include performance measurement, security provisions, service charge amount and metering method, exit strategy (how to terminate contract), etc. Therefore, SLA is a key objective to be audited.

Finally, cloud computing auditors need to be knowledgeable regarding all aspects of cloud computing. As we mentioned above, the future of cloud computing auditing faces a number of challenges. The auditing firm must well prepare their IT auditors to face these challenges by offering sound educational/training programs. A better way to develop their auditors may be through the creation of a knowledge management system (KMS) for cloud computing audits. All senior cloud computing auditors' knowledge, problem solutions, and work experience can be stored in the KMS for easy access.

8. Conclusion

Cloud computing is broadly accepted in the IT industry. Its development brings in benefits such as cost saving, ease of use, scalability, flexibility, and environmental sustainability. This new technology adds value to the society, however, it is like a giant that may not be easy to handle, especially with regard to IT auditing practices.

In order to understand the inner insinuation of this new area, this paper conducts a study to investigate the implications of IT auditing, cloud computing, and cloud computing auditing. After examining the development horizon, this paper lays down a number of challenges that face the field of cloud computing, including technological complexity, security risk, its weaknesses and immaturity, lack of cloud computing audit standards, and contractual issue such as SLA. A future development issue could be knowledge worker's training and knowledge management system's construction.

We wish that this study could provide some guidance to those IT auditors who are going to conduct cloud computing audits in the near future.

References

[1] J. Akoka, I. Wattiau, A framework for auditing web-based information systems, ECIS 2010 Proceedings. Paper 58, 2010.

[2] D.C. Chou, An investigation into IS outsourcing success: the role of quality and change management, Int. J. Inf. Syst. Chang. Manag. 2 (2) (2007) 190–204.

[3] D.C. Chou, A.Y. Chou, Integrating change management and change auditing into information technology consulting practice, Int. J. Inf. Syst. Chang. Manag. 4 (1) (2009) 15–41.

[4] D.C. Chou, A.Y. Chou, Information systems outsourcing life cycle and risks analysis, Comput. Stand. Interfaces 31 (5) (2009) 1036–1043.

[5] D.C. Chou, A.Y. Chou, Analyses of software quality and auditing, in: C.V. Brown, H. Topi (Eds.), IS Management Handbook, seventh editionCRC Press, Boca Raton, FL, 2000.

[6] D.C. Chou, Cloud computing: A value creation model, Comput. Stand. Interfaces 38 (2015) 72–77.

[7] CDW, Migrating to the Cloud, a white paperAvailable at http://cdw.com/cloud2012 (accessed on November 1, 2012).

[8] J. Cross, IT outsourcing: British Petroleum's competitive approach, Harv. Bus. Rev. (May-June 1995) 95–102.

[9] H. Du, Y. Cong, Cloud computing, accounting, auditing, and beyond, CPU J. (October 2010) 66–70.

[10] M.J. Earl, The risks of outsourcing IT, Sloan Manage. Rev. (Spring 1996) 26–32.

[11] S. Fraser, The Risk Based Audit Processavailable at http://www.charteredaccountants.com.au/News-Media/Charter/Charter-articles/Audit-and-assurance/2011-07-The-Risk-Based-Audit-Approach.aspx2012 (accessed on November 1, 2012).

[12] S. Gadia, Cloud computing: an auditor's perspective, ISACA J. 6 (2009) (http://www.isaca.org/Journal/archives/2009/Volume-6/Pages/Cloud-Computing-An-Auditor-s-Perspective1.aspx).

[13] S. Gadia, Cloud computing risk assessment: A case study, ISACA J. 4 (2011) (http://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx).

[14] S. Hamm, Cloud computing's big bang for business, Bus. Week 15 (June 2009) 42–44.

[15] J.A. Hall, Information Technology Auditing and Assurance, third edition South-Western Cengage Learning, Mason, OH, 2011.

[16] G. Hutchins, Value-Based Auditing: Your Best Assessment Toolavailable at http://www.qualitydigest.com/oct02/articles/04_article.shtml2012 (accessed on November 1, 2012).

[17] Institute of Internal Auditors (IIA), Available at http://www.theiia.org2012 (accessed November 1, 2012).

[18] ISACA, ISACA Issues Four New Audit Programs on Cloud Computing, Crisis Management, Security and Active DirectoryAvailable at http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-Issues-Four-New-Audit-Programs-on-Cloud-Computing-Crisis-Management-Security-and-Active-Directory.aspx2010.

[19] M.C. Lacity, R. Hirschheim, Information Systems Outsourcing, John Wiley & Son, New York, 1993.

[20] J.W. Merhout, D. Havelka, Information technology auditing: A value-added IT governance partnership between IT management and audit, Commun. Assoc. Inf. Syst. 23 (2008) (Article 26. Available at: http://aisel.aisnet.org/cais/vol23/iss1/26. Accessed June 05, 2012).

[21] P. Mell, T. Grance, NIST definition of cloud computing, NIST Special Publication 800-1452011.

[22] NIST, NIST Cloud Computing Programavailable at http://www.nist.gov/itl/cloud/2012 (accessed November 01, 2012).

[23] C.A. Nicolaou, A.I. Nocolaou, G.D. Nocolaou, Auditing in the cloud: Challenges and opportunities, CPA J. (January 2012) 66–70.

[24] M. O'Leary, The mainframe doesn't work here anymore, CIO 6 (6) (1990) 77–79.

[25] V. Raval, Risk landscape of cloud computing, ISACA J. 1 (2010).

[26] K. Robson, C. Humphrey, R. Khalifa, J. Jones, Transforming audit technologies: Business risk and the audit field, Acc. Organ. Soc. 32 (2007) 409–438.

[27] S. Ross, Cloudy daze, ISACA J. 1 (2010).

[28] T.W. Singleton, IT audits of cloud and SaaS, ISACA J. 3 (2010) 1–3.

[29] R. Coase, The nature of the firm, Economica 4 (1937) 386–405.

[30] O.E. Williamson, The modern corporation: origin, evolution, attributes, J. Econ. Lit. 19 (1981) 1537–1568.

[31] M. Porter, Competitive advantage: Creating and sustaining superior performance, The Free Press, New York, NY, 1985.

[32] K.R. Conner, A historical comparison of resource-based theory and five schools of thought within industrial organization economics: Do we have a new theory of the firm? J. Manag. 17 (1) (1991) 121–154.

[33] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing - the business perspective, Decis. Support. Syst. 51 (2011) 176–189.