JOURNAL OF INFORMATION SYSTEMS
Vol. 26, No. 2
Fall 2012
pp. 13–33

American Accounting Association
DOI: 10.2308/isys-50229

Cloud Computing: Overview and Risk Analysis

Fatima A. Alali
Chia-Lun Yeh
California State University, Fullerton

ABSTRACT: We provide an overview of cloud computing: evolution, benefits, and challenges. Then we examine the risk characteristics identified in accounting and auditing literature by comparing a hand-collected sample of cloud computing companies with a matched sample of non-cloud computing companies. The study uses a comprehensive set of factors used in accounting and auditing literature to describe client business risk, audit risk, and auditor-related risk. Unsurprisingly, the findings show that large companies in the historically high-risk information technology industries provide cloud computing. More interestingly, the results show that cloud computing is more leveraged, and more likely to have a material weakness and longer audit tenure. Cloud computing companies are also more likely to restate their financial statement after providing cloud technologies. Some of the risk variables we used in the study are not statistically significant in capturing the risks of cloud providers (e.g., security, privacy, availability, confidentiality). The study contributes to the literature in IT outsourcing in general, and in cloud computing more specifically. The study also responds to the recent call for insightful research in cloud computing.

Keywords: cloud computing; risk characteristics; accounting and auditing research.

I. INTRODUCTION

The objective of the study is twofold. First, we provide an overview of cloud computing, including a definition, the evolution, and benefits and challenges. Second, we build on existing literature in accounting and auditing to examine risk characteristics of companies that develop or provide servers, applications, platforms, and/or infrastructure technologies for cloud computing. The study is motivated by the increasing use of cloud computing and the evolving related-business models that expose managers and auditors to increased risks (Singleton 2010). In addition, the study is motivated by the lack of research on cloud computing (Grabski et al. 2011). The idea of cloud computing as a utility was first introduced by McCarthy (1961) and subsequently explored by Licklider (1963), who pursued a globally accessible computer network.

Cloud technology has evolved from the costly and complex information technology (IT) solutions and enterprise applications in the 1980s, and is enabled by the recent expansion of the

We are grateful for the insightful comments from Miklos A. Vasarhelyi (editor) and three anonymous referees.
Editor's note: Accepted by Miklos A. Vasarhelyi.

Published Online: June 2012

Internet in the 1990s. Moreover, the dramatic drop in the bandwidth costs and other technological advances have contributed to the emergence of cloud computing (Grabski et al. 2011; Mohamed 2009). Unlike previous generations of application service providers (ASPs), cloud computing provides tangible and measurable business benefits by allowing multi-user-real-time access without the up-front investment cost (ISACA 2009a). Today, cloud computing is used in a multitude of business applications and processes. However, the complexity and diversity of cloud computing architecture, coupled with the separation of data ownership and data controls, possible disruption of service, and data recoverability, create challenges for the assessment and management of these risks by both managers and auditors (Blaskovich and Mintchik 2011).

The study highlights the role of standardization in mitigating risks and how audit tools have changed over time to accommodate the evolution of technology. Standardization creates a level playing field and provides clear guidance to mitigate risks. In mid/late 2011, an agreed-upon definition of cloud computing and a roadmap for cloud standards were established (Hogan et al. 2011; Jansen and Grance 2011). The National Institute of Standards and Technology (NIST) defines 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" (Jansen and Grance 2011, 11). This definition provides the essential characteristics of cloud computing: on-demand self-service, broad-network access, resource pooling, rapid elasticity, and measured service.

The NIST also identifies three cloud service models and four cloud deployment models. The service models are:

(1) Software-as-a-Service (SaaS) allows users to run a variety of software applications on the Internet without having possession or managing applications (e.g., Salesforce.com, Gmail, Microsoft Online).
(2) Platform-as-a-Service (PaaS) provides a computing platform to support building of web applications and services completely residing on the Internet (e.g., Google Apps, Force.com, 3Tera AppLogic).
(3) Infrastructure-as-a-Service (IaaS) allows the use of computer hardware and system software, including operating systems and communication networks in which the cloud provider is responsible for hardware installation, system configuration, and maintenance (e.g., Amazon EC2, Citrix Cloud Center).

The deployment models are:

(1) **Public cloud** is available to the public or a large industry group and is owned by an organization selling cloud services.
(2) **Private cloud** is a cloud operated solely for an organization. It can be managed by the organization or a third party and can exist on or off premises of the organization.
(3) **Community cloud** is a cloud that is shared by several organizations and supports a specific community purpose (e.g., mission, security requirements, policy, and compliance). It can be managed by either an organization or a third party and can be on or off premises of the community organizations.
(4) **Hybrid cloud** is a composition of two or more clouds that remain unique entities but are bound by standardized or proprietary technology that enables data and application portability (Jansen and Grance 2011).

Regulatory bodies are also developing standards and guidance on cloud technologies. For example, in December 2011, COSO released an exposure draft to update COSO's Internal Control Integrated Framework due to the evolving role of technology in business and the emergence of

complex fast-changing technologies. In its exposure draft, COSO addresses the complexity of the technology infrastructure (e.g., communication networks, computing resources, applications) shared by different business units within an organization (e.g., shared service center), or outsourced to a third-party service organization or a location-independent technology service (cloud computing). It provides means to identify, analyze, and manage risks by grouping entity objectives for each component of the COSO Framework into operating, financial, and compliance objectives, and subsequently subcategorized them into principles. Controls are placed to track technological changes, and assess and respond to existing and new risks.[1] The AICPA has also issued assurance guidance on the internal controls at service organizations to controls related to security, availability, processing integrity, confidentiality, and privacy due to changing technologies. Accounting and auditing practices have also developed technologies to manage and audit these technologies (Singleton 2010; Ross 2010).

Prior academic studies extensively examine the effect of IT and IT outsourcing on audits (e.g., Glover et al. 2001; Kotb and Roberts 2011; Sutton and Hampton 2003; Janvrin et al. 2008; Sutton 2006; Wright and Wright 2002). However, there is scarce academic research addressing emerging technologies (Grabski et al. 2011). This study adds to the research by using variables identified in prior studies (i.e., Johnstone 2000; Elder et al. 2009)[2] to examine risk characteristics of cloud computing companies. We collect a sample of companies that provide cloud technologies. We then obtain a non-cloud sample, and use univariate and logistic regression to analyze differences between cloud and non-cloud companies.

The empirical results show that cloud providers fall in historically high litigation industries (Francis et al. 1994). The study shows that compared to non-cloud companies, cloud companies are highly leveraged, less liquid, and more likely to have internal control material weaknesses. Cloud providers also have longer auditor tenure. Compared to the pre-cloud period, cloud providers have become highly leveraged, less liquid, and more likely to restate their financial statements. However, other variables characterizing client business risk and audit risk used in the study are not statistically significant. These results show that although cloud technology exposes auditors and clients to increased risks and challenges (Singleton 2010; Ross 2010), several risk variables used in this study fail to capture these challenges. These results may be driven by the small sample size.

This study contributes to the extant literature in the following ways. First, the study responds to the call for additional research in emerging technologies affecting accounting and audit practice, especially cloud technologies (Blaskovich and Mintchik 2011). Second, cloud computing is attracting large companies such as Apple, Amazon, and Google to compete, and more companies are expected to use or provide this technology in the future.[3] Cloud computing companies fall in historically high litigation industries (e.g., high technology). However, as discussed in detail in subsequent sections, risks are higher inherently for cloud companies in these industries relative to other companies in the same industries. Therefore examining cloud providers is important, although our results are supportive of some risk measures but not others.

---

[1] However, COSO (2011, 20) does not state internal controls policies, procedures, and processes to identify, assess, and manage risk specifically in a cloud environment. It codifies the control concepts from the original framework into 17 principles and 82 associated attributes. It proposes a principle-based approach to internal controls and identifies where technology must be considered, especially due to the role of evolving business models and technological advances.

[2] Because we are aiming at capturing risk characteristics between cloud and non-cloud companies, and because this is an empirical study based on publicly available data in companies' annual reports, Audit Analytics, and Compustat databases, we selected variables that are used in empirical studies to capture client risk and audit risk. We use Johnstone (2000) and Elder et al. (2009) to compile a comprehensive list of variables that captures client business risk and audit risk.

[3] Gartner Research (2011) shows that the cloud service industry is growing through 2014, when worldwide cloud service revenues are predicted to reach $148.8 billion.

Third, this is the first study that hand-collected data on companies that provide cloud technologies to examine risk characteristics identified in prior studies. Studying cloud's risk characteristics is important because service organizations provide cloud services to audit clients. Fourth, the study shows that some of the risk variables are not significant. This may indicate that cloud providers' risk characteristics (e.g., security, availability, confidentiality) are not captured by variables or that these variables are not good measures of risk constructs. Thus, we call for additional research using qualitative research methods, and perhaps larger samples to better empirically capture cloud risk constructs.

The subsequent sections are organized as follows: Section II elaborates on cloud computing benefits, challenges, and the role of standardizations. Section III provides a literature review on cloud computing studies and IT outsourcing studies. Section IV presents data collection, Section V presents the statistical model, and Section VI discusses the findings. Section VII concludes the study and provides areas for future research.

II. CLOUD COMPUTING: EVOLUTION, BENEFITS, CHALLENGES

In this section, we provide an overview of cloud computing, its benefits and risks. We also discuss the role of standardization mitigating risks.

Evolution

The use of computers for business data processing began in the 1960s with the early third-generation mainframe computers. The subsequent increase in I/O bandwidth and the emergence of client server applications in the 1980s, followed by the rise of the Internet in the 1990s, led to web-based applications and e-commerce platforms. Advances in grid computing allowed for efficiently performing computationally intensive tasks (Shroff 2010). Application service providers (ASPs) offered software packages within users' organizations over the Internet. Early successful ASPs include Intuit hosting QuickBooks, a desktop accounting solution, and Salesforce.com hosting a customer relationship management (CRM) solution. Subsequently, new applications were created from scratch using web-based architecture, referred to as Software-as-a-Service. Salesforce.com enabled end users to customize the functionality of their view of the application, allowing them to save time and cost. The ability of users to customize application functionality was extended to cover other applications features. This allowed users to create applications using the same host (SaaS platform). Later, a scripting language was added to position these features as an independent-hosted development platform and thus the emergence of PaaS (Shroff 2010). In the 2000s, using virtualization many logical operating systems were enabled to share a single physical machine resource.

Amazon exploited virtualization to meet efficiently and effectively its demand fluctuations by launching S3 (simple storage system) and EC2 (elastic computer cloud), where users could rent storage and compute on Amazon servers. Moreover, Amazon made available its own system software tools such as Amazon SQS (simple queue service) and SimpleDB (a non-relational database). Amazon's cloud is an IaaS. Google developed a distributed model to support its complex voluminous computational issues relating to large-scale web indexing, voluminous searches, and machine-learning targeted advertisements. The Google cloud, known as Google App Engine, is a PaaS.

The above discussion shows how cloud computing evolved from the technologies used in mainframes to virtualization. Although ASPs have similar characteristics to subsequent generations of SaaS and cloud computing, ASPs provide limited customization choices. SaaS is developed from the ground up; it is hosted by an SaaS vendor and the user accesses it over the Internet. Unlike the ASPs that required users to install the software on their computers, the SaaS user does not buy the software, but pays a fee per use. SaaS also allows multi-tenants, so multiple users can use the service at the same time from different locations over the Internet. The evolution from mainframes

to cloud computing provides multiple benefits and exposes challenges. We next discuss benefits and challenges of cloud computing.

Benefits and Challenges and the Role of Standardization

Cloud computing provides several benefits. One of the main drivers of corporate interest in cloud computing is the reduction in capital investments. The investment in IT represents an average of 50 percent of capital expenditure budgets (U.S. Department of Commerce 2008). However, cloud computing allows companies to tie their costs to their revenues as incurred, depending on the seasonal demands of their end users' businesses (KPMG 2010). Cloud providers allow a certain level of flexibility in resources depending on cloud users' operations (Armbrust et al. 2010), and thus users avoid the risks of over-provision (i.e., waste of resources) and under-provision (i.e., loss of potential revenues) due to uncertain business flow.[4] In addition, necessary resources can be gathered within a short time and underlying infrastructures for specific projects can be configured in a few days (Youseff et al. 2009). The flexibility and rapid adjustment of cloud computing enable companies to test as many strategies and products as possible, and thus identify multiple profitable strategies and products (Garland et al. 2010). Additionally, the pricing models, which are based on units of resources acquired, to some extent relieve the users from the costs of these services. The up-front costs for some services may be eliminated as well (Armbrust et al. 2010). Other costs include developing a virtual machine (VM) algorithm to define efficient and effective allocation of resources (Buyya et al. 2009).[5]

Cloud technology subjects both providers and users to multiple challenges and risks. In response to security risks, the NIST created a cloud computing security working group to assist corporations in developing data security policies and governance systems. To enhance cloud security, W3C recommends the use of XML signatures to sign data or any resource of any type, typically XML documents, and anything that is accessible via a URL. Furthermore, NIST has published a list of security and authentication protocols, such as XML Encryption Syntax and Processing, Transport Layer Security (TLS), Key Management Interoperability Protocol (KMIP), and Security Content Automation Protocol (SCAP) for cloud computing.[6] The NIST continues to provide guidance on cloud computing (Jansen and Grance 2011) and develop standards (Hogan et al. 2011).

In addition, cloud providers have designed and implemented controls to assess and manage cloud risks. For example, Harauz et al. (2009) highlight the importance of data confidentiality, integrity, and availability. They suggest storage providers should at least meet two requirements: (1) encryption schema should be applied to protect all data stored in the devices, and well-defined controls should be implemented to prevent unauthorized access; and (2) cloud providers should schedule regular data backup and safe storage of the backup media. The recent cloud outage at Amazon and Microsoft shows the significance of backup and emergency plans. In addition, service level agreements (SLAs)[7] can be used to define roles and responsibilities of cloud providers and users to assure availability and retrievability.

---

[4] Moreover, from the cloud provider's view, with cloud computing, the cost of using one thousand servers for one hour is no more than that of using one server for a thousand hours. This feature allows the pricing offered to end users to be more flexible. In addition, cloud computing provides users the flexibility to use multiple servers to utilize the cloud service without incurring abnormal costs. At the same time, the efficiency of cloud users' services increase, thus allowing for better business flows (Armbrust et al. 2010).

[5] For more detailed literature review on these topics, refer to Garland et al. (2010), Harauz et al. (2009), Pearson (2009), and Armbrust et al. (2010).

[6] Moreover, the NIST provides a list of other standards and W3C-recommended technologies to ensure security, authentication, integrity, and confidentiality. Refer to NIST (2012) for a list of these standards and their applicability.

[7] SLAs are agreements between cloud providers and cloud users defining issues related to usage, availability, and recoverability.

Other studies recommend ways to improve data privacy and security. Pearson (2009) recommends the use of Privacy Impact Assessment (PIA), launched by the U.K. Information Commissioners Office (ICO) to assess the level of privacy risk. PIA would be applied in the early stages of design process so that if privacy risk is unacceptable, design settings may be changed to accommodate the risk. Privacy requirements are examined and altered at different cloud lifecycles. Companies may use Privacy Enhancing Technology (PET). The U.K.'s Information Commissioner's Office (2008) in Pearson (2009, 5) defines PET as "any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998."

Cannon (2004) suggests engineers adjust designs or features of clouds for privacy considerations, and all subsequent changes are to be recorded as information technology change management. As a result, audit trails are maintained. Cloud providers must demonstrate the existence of effective security and privacy controls, data retrievability, and that the cloud is in compliance with trans-border laws, especially if information can be stored anywhere (Vael 2010). The above discussion shows the importance of internal controls to mitigate cloud risks. Both information systems and accounting researchers have also examined IT outsourcing, cloud security controls, and how auditors assure compliance with regulations. In the next section, we present prior studies that examined the effect of IT and IT outsourcing on the conduct of audits.

III. LITERATURE

Limited regulatory guidance is available to support and guide cloud computing for both cloud providers and users. Existing regulations include an IT internal control framework (ITGI 2005), the COSO Framework, and audit of internal controls of service organizations through SAS 70 (AICPA 1992) and SSAE 16.[8] SAS 94 (AICPA 2001) and Auditing Standard No. 5 (PCAOB 2007) affirm that the nature and character of an entity's use of technology in its information system affects the entity's overall internal control structure. These standards require auditors to understand business processes and internal controls to assess risks of material misstatements in the financial statements, as well as identify control deficiencies and material weaknesses in internal controls. Singleton (2010) provides that IT auditors need to understand cloud technology, especially SaaS and IaaS; establish an approach for identifying key risks; and develop effective audits. Material weaknesses identified at the cloud provider also affect the cloud users and their businesses. The infrastructure outsourcing in the context of cloud computing affects multiple or sometimes all business processes, including sales, purchasing, production, customer relations, supplier management, and payroll (Gill 2011; DeFelice 2010; Du and Gong 2010).

Singleton (2010) propose a risk-based approach that encourages effective risk assessment and auditing for the identified risks. Ames and Brown (2011) identify categories of cloud risks as related to governance and ownership, data security policies, data safeguarding, access and identity controls, network/communication/insecure application programming interfaces, service level agreement and contract management, compliance risks, and vendor management. These risks not only affect cloud providers, but also contribute to business processes at the cloud user's place of business.[9] Other studies also examine how managers and auditors should address these cloud computing

[8] SSAE No. 16, reporting on Controls at a Service Organization, supersedes the guidance for service auditors in AU 324 on service organizations, when the service auditor is reporting on periods ending on or after June 15, 2011. Under the new rules, SOC examination involves rigorous tests of controls as related to: the physical and hardware components of a system (infrastructure); the programs and operating software of a system, including applications and utilities (software); the personnel involved in the operation and use of a system, including developers, operators, users, and managers; and data including transaction streams, files, databases, and tables (AICPA 2011).

[9] For a detailed description of these risk exposures, please refer to Ames and Brown (2011).

complexities and risks as governance/compliance practice (ISACA 2009b, 2010) or assurance service (e.g., Knolmayer and Asprion 2011; Davis et al. 2006; Moeller 2010).

Research from practice discussed above shows that cloud technology makes the IT environment more complex and brings along unique challenges. Related to this literature, academic research examined audit issues in IT and outsourced IT environments. Technology-based businesses have new features, risks, and controls that change the client's risk profile (Glover et al. 2001; Kotb and Roberts 2011). These new risks can be classified as legal risks (Sutton and Hampton 2003; Billing 2001) and IT risks (Glover et al. 2001). Cash et al. (1977) provided one of the earliest approaches for auditing EDP-based accounting information systems (AIS). More recently, Ahn et al. (2001) proposed a framework for auditing ASPs, starting with a framework to audit the network, data center, and application, and assuring monitoring and security controls.

Other studies concerning ERP environments (Sutton and Hampton 2003; Sutton 2006) show that complex technologies may have significant financial reporting implications and that their outsourcing requires the auditor to redefine the boundaries of the client to include the inter-organizational relationships that represent trading partners in the supply chain and the electronically connected business partners. Similarly, Wright and Wright (2002) posit that ERP systems present several unique control risks due to the implementation processes that may have significant impact on system reliability, ongoing risk variation across applications and vendors, and the increasing need to test the process rather than the output. Curtis et al. (2009) indicate that these represent challenges for auditors.

Grabski et al. (2011) provide a literature review of ERP research and cite multiple studies that encourage a move toward continuous auditing (Zhao et al. 2004; Liang et al. 2001; Rezaee et al. 2001; Chou and Chang 2010; Kuhn and Sutton 2010). Internal controls related to security and compliance are critical to evaluate. Computer Assisted Auditing Techniques (CAATs) developed for an ERP environment provide powerful tools for an auditor to formalize audit procedures and audit judgment (Kilpatrick 2000; Deshmukh 2006; Westervelt 2006; ACL 2010; Alles et al. 2006). Other studies show that ERP embedded audit modules (EAMs) offer effective fraud prevention in an ERP environment (Debreceny et al. 2005), while Pathak and Lind (2010) suggest new IT-driven audit techniques and tools for web-based businesses.

On the other hand, studies such as Janvrin et al. (2008) show that IT specialists are used less frequently and that auditors' use of digital analysis, expert systems, tests of online transactions, database modeling, and continuous transaction monitoring are less used in an IT audit environment. Consistent with these results, Curtis et al. (2009) provide that IT auditors spend fewer hours in audit engagement compared to five years ago, and that CPA firms rely more on clients or consultants hired by the client for controls testing.[10] Taken together, the studies above document a wide range of auditor responses to clients' IT outsourcing. As emerging regulations become effective (e.g., COSO 2011; AICPA 2011), both auditors and managers will take critical steps, probably by using innovative technologies to assess and manage cloud computing risks to global changing business models.

IV. DATA COLLECTION

We use the LexisNexis academic search function to search the annual reports (10-Ks) filed with the Securities and Exchange Commission (SEC) for keywords such as "cloud" or "cloud computing" for periods on and after January 1, 2006, to December 31, 2008.[11] The search resulted

[10] Curtis et al.'s (2009) results are based on discussions with two partners at Big 4 firms.

[11] We selected this time period because of recent use and development of cloud technologies. A few companies indicated in their 10-Ks that they started providing cloud technologies in 2006 or 2007 and continue to do so in 2008 and 2009.

in 166 hits. Cloud companies are identified as those that provide services as infrastructure or platform, or are cloud users/application providers. As a result, the cloud providers sample includes 67 companies. We further obtain financial accounting and audit variables from Compustat and Audit Analytics for the period 2006–2009 as available at the time of this research. Moreover, we collect financial accounting and audit variables for the matched companies as the control group based on year, industry, and total assets. We exclude companies with missing data, and the final testable sample includes 370 firm-year observations over the period 2006–2009. Our final cloud sample includes 67 firm-year observations identified in the post-cloud period, 118 firm-year observations in the pre-cloud period, and 185 firm-year observations identified as a non-cloud sample.

Table 1, Panel A shows the pooled sample distribution by year. The sample is evenly distributed across 2006–2009, with about 25 percent of firm-year observations in each year.[12] Panel B shows that 67 percent of cloud companies fall in 2009, 24 percent in 2008, and 9 percent in 2006–2007. Panel C of Table 1 shows the distribution of the cloud companies sample by SIC industry classification. About 43 percent of the cloud companies are in the prepackaged software industry. These companies provide SaaS in cloud technology. More than 10 percent of the cloud companies are in the business services industry, including companies such as Savvis Inc., which provides information technology services including co-location services and cloud services. More than 16 percent of cloud companies are in the communication and computer communication industry, 10.45 percent are in the computer equipment and peripherals industry, 8.96 percent are in programming, and 4.4 percent are in computer storage industries. About 5.97 percent of cloud companies are in the computer integrated system and computer processing industry.

Panel D of Table 1 shows that 70 percent of the pooled sample is audited by Big 4 auditors (259 firm-year observations), while 17.37 percent (45/259) of cloud companies are audited by Big 4 auditors in the post-cloud period; nearly 32.82 percent (85/259) of the cloud companies were audited by Big 4 auditors in the pre-cloud period. Of the 67 firm-year cloud observations, 67.16 percent (45/67) are audited by Big 4 firms, compared to 32.84 percent (22/67) audited by non-Big 4 auditors. In the non-cloud sample, about 50 percent of the companies are audited by Big 4 auditors.

IV. MODEL DEVELOPMENT

The nature of cloud technology imposes particular types of risks (Singleton 2010; Ames and Brown 2011). However, because data are not publicly available at a detailed level, we use risk characteristics identified in Johnstone (2000) and Elder et al. (2009). These risks are categorized into client business risks and audit risks. Therefore, the following model is developed:[13]

[12] The cloud sample includes 185 firm-year observations, of which 184 firm-year observations of cloud firms have three or four years of data. Only one cloud company has one year of data. The control sample follows the same pattern.

[13] The variables used in Johnstone's (2000) study are based on a survey questionnaire. Therefore, we substitute for certain variables by well-agreed-upon definitions. For example, short-term financial liquidity is measured by operating cash flows divided by total assets, while the company's inherent risk is measured by the sum of accounts receivables and inventory divided by total assets. In addition, we substitute for some of the variables from Elder et al. (2009) as follows. We include the *ERRORD* variable that equals 1 if a company has reported one or more accounting errors and 0 otherwise, and the *MWD* variable that equals 1 if a company reported one or more material weakness(es) in the internal controls audit and 0 otherwise, and the *MWD*. We use the count of weaknesses and number of accounting errors in Audit Analytics. Our results are robust to alternative definitions of entity-level internal control weakness(es) and accounting misstatements. Only a few companies had stricter definitions of material weakness and accounting misstatements so as to find significant results.

TABLE 1

Sample Distribution

Panel A: Pooled Sample Distribution by Fiscal Year

Fiscal Year	Number of Companies	Percent of Companies
2006	92	24.86%
2007	92	24.86%
2008	94	25.41%
2009	92	24.86%
Total	370	100.00%

Panel B: Cloud Companies Sample Distribution by Year

Fiscal Year	Number of Cloud Companies	Percent of Cloud Companies
2006	2	2.99%
2007	4	5.97%
2008	16	23.88%
2009	45	67.16%
Total	67	100.00%

Panel C: Cloud Companies Sample Distribution by Industry

Industry	Number of Cloud Companies	Percent of Cloud Companies
Prepackaged Software	29	43.28%
Communications Equipment, Computer/ Telephone Communication	11	16.42%
Business Services	7	10.45%
Computer and Office Equipment and Peripherals	7	10.45%
Computer Programming Services	6	8.96%
Computer Integrated System and Computer Processing	4	5.97%
Computer Storage Devices	3	4.48%
Total	67	100.00%

Panel D: Pooled Sample Distribution by Type of Auditors

	Big 4	Non-Big 4	Total
Non-Cloud Companies	129	56	185
Cloud Companies	45	22	67
Pre-Cloud Adoption	85	33	118
Total	259	111	370

$$\begin{aligned} Cloud\_Tech = {} & \beta_0 + \beta_1 Size + \beta_2 Liquidity + \beta_3 Leverage + \beta_4 ROA + \beta_5 Z\text{-}Score + \beta_6 Segment \\ & + \beta_7 Loss + \beta_8 Merger + \beta_9 Litigation\_Risk + \beta_{10} AudFees + \beta_{11} Going\_Concern \\ & + \beta_{12} Big4 + \beta_{13} Tenure + \beta_{14} Inherent\_Risk + \beta_{15} |DACC| + \beta_{16} Restatement \\ & + \beta_{17} SEC404 + \beta_{18} ERRORD + \beta_{19} MWD + \beta_{20} ARL + \beta_{21} December \\ & + \beta_{22-24} D2006 - D2008, \end{aligned} \tag{1}$$

where all variables are defined in Table 2.[14]

Dependent Variable

In the logistic regression, the dependent variable is *Cloud_Tech*, which is an indicator variable equal to 1 if company is cloud, and 0 otherwise. The control sample includes the non-cloud companies. We alternatively define *Cloud_Tech* as 1 if a cloud company is in the post-cloud period, and 0 if it is in the pre-cloud period, and run separate analysis.

Independent Variables

Following Johnstone (2000) and Elder et al. (2009), we incorporate different categories of risk variables. Moreover, we add two other control variables—one for audit report lag (*ARL*) and one for fiscal year-end. We include *ARL* because it captures other complexity and risks factors that are not accounted for by other control variables. *ARL* is calculated by the number of days between fiscal year-end and the date of auditor signature on the auditor's report. We include *December* as an indicator variable because the majority of companies in our sample are international companies and thus are more likely to have a December fiscal year-end to meet international statutory requirements. Therefore, this variable also controls for other complexity factors.

The coefficients of *Size*, *Leverage*, and *Litigation_Risk* are expected to be positive. Cloud computing companies are expected to be large software and technology companies that have financial and infrastructure capabilities to provide cloud services. These cloud services may require additional investments funded by an increase in debt and/or equity. Moltzen (2010) suggests that cloud companies have significant amounts of debt (e.g., Terremax, Equinix), while others suffer a downward debt rating (e.g., Qwest).

The coefficients of *ROA* and *Loss* reflect the profitability of cloud companies compared to non-cloud companies. Cloud companies may be able to generate positive profits, and thus *ROA* is expected to be positive and *Loss* to be negative. However, most of the cloud companies in the sample started providing cloud technologies in 2008–2009 and thus the positive effect on net income may have not yet been realized. Therefore, the coefficients of *ROA* may be negative and *Loss* may be positive.

The coefficient of *Liquidity* is expected to be negative as measured in terms of cash flows from operations. It is unlikely that a company will generate positive cash flows after implementation, but rather companies take time to market cloud computing and sell their services to generate positive cash flows. Media reports indicate that cloud computing is not well marketed (even in companies such as Google). While these companies continue to spend on infrastructure and building partnerships to reduce investment costs and increase revenues, positive cash flows may be lagging. These factors also

[14] Due to perfect multicollinearity between *IC_Opinion* and *MWD*, we omit the former in the logistic regression model. We also omit *Audchange* from the logistic regression model because only 18 companies changed auditors during the sample; nine were cloud and nine were non-cloud companies. Including auditor changes in the regression do not change the results. Excluding *ARL* and *December* variables provides materially the same results.

TABLE 2

Variable Definitions

Variable	Definition
Dependent Variable	
Cloud_Tech	Indicator variable equals 1 if cloud computing company, and 0 otherwise; alternative definition also used where 1 if post- cloud and 0 if pre-cloud.
Independent Variables	
Client Business Risk Variables	
TA[a]	Total assets.
Size	Log of total assets.
Liquidity	Cash flow from operations/total assets.
Leverage	Debt-to-equity ratio.
ROA	Income before extraordinary items/total assets.
Z-Score	(EBIT/Total Assets) $*$ 3.3 + (Net Sales/Total Assets) $*$ 0.99 + (Market Value of Equity/Total Liability) $*$ 0.6 + (Working Capital/Total Assets) $*$ 1.2 + (Retained Earnings/Total Assets) $*$ 1.4 (following Altman [1968]).
Segment	Log (1 + Segment).
Loss	Indicator variable equals 1 if income before tax is negative, and 0 otherwise.
Merger	Indicator variable equals 1 if merger occurred in a company, and 0 otherwise.
Litigation_Risk	Indicator variable equals 1 if company is in the following SIC code: 2833–2836, 8731–8734, 3570–3577, 7370–7374. 3600–3674, and 5200–5961, and 0 otherwise (following Francis et al. [1994]).
Auditor-Related Variables	
Audit_Fee[a]	Audit fees (un-scaled).
Non_Audit_Fee[a]	Non-audit fees (un-scaled).
AudFees	Audit fees scaled by audit and non-audit fees.
NonaudFees[a]	Non-audit fees scaled by audit and non-audit fees.
Going_Concern	Indicator variable equals 1 if a company received a going concern opinion, and 0 otherwise.
Audchange[a]	Indicator variable equals 1 if a company changed auditors, and 0 otherwise.
Big4	Indicator variable equals 1 if company audited by a Big 4, and 0 otherwise.
Tenure	Indicator variable equals 1 if auditor's tenure is less than three years, and 0 otherwise.
Audit Risk Variables	
Inherent_Risk	Accounts Receivable + Inventory/Total Assets
$\|DACC\|$	The absolute value of *DACC*. *DACC* is the residual from $TOTACCi, t = \beta_0 (1/Tai, t-1) + \beta_1 (\Delta SALESi, t - \Delta ARi, t)/TAi, t-1 + \beta_2 (PPEi, t/TAi, t-1)$ (following Kothari et al. [2005] and Elder et al. [2009]).
Restatement	Indicator variable equals 1 if a company restated its financial statements, and 0 otherwise.
SEC404	Indicator variable equals 1 if company reported under SOX Section 404, and 0 otherwise.
ERRORD	Indicator variable equals 1 if a company reported an accounting error due to internal control deficiency/material weakness, and 0 otherwise.

(continued on next page)

TABLE 2 (continued)

Variable	Definition
Dependent Variable	
MWD	Indicator variable equals 1 if a company has two or more material weakness(es) in its internal controls, and 0 otherwise.
Other Control Variables	
ARL	Log of audit reporting lag, which is the difference between auditor report date and the fiscal year-end of a company.
December	Indicator variable equals 1 if a company has a December 31 fiscal year-end, and 0 otherwise.
D2006–D2009	Indicator variables representing fiscal years 2006–2009.

[a] Only included for descriptive statistics.

affect profitability and liquidity. Additionally, the coefficients of *Z-score* and *Going_Concern* indicate financial difficulties upon providing cloud services, especially that accruing the benefits of cloud computing may take time to improve profitability and generate cash flows.

Cloud companies may have a larger number of segments (*Segment*) and/or be involved in mergers (*Merger*). However, most services are provided through the Internet and thus also result in reducing business complexity as measured by the traditional number of segments and/or mergers. Cloud computing mergers, however, are unlike traditional mergers and acquisitions. This is because there is less concern about the "booked revenue or other traditional metrics, and more about market influence and speed to market." Cohen (2009). He describes a mini-merger of a company and an idea or acquisition of research and development, as opposed to more traditional mergers.[15]

The coefficient of *Big4* is expected to be positive. The majority (about 67 percent) of cloud companies in the sample are audited by Big 4 auditors, which may be due to the requirements of internal control audits and the notion that Big 4 auditors have the capabilities to audit the largest public companies. The coefficient of *Tenure* is expected to be negative, as cloud companies are larger in size and thus are expected to have a stable relationship with their auditors, while the adoption of cloud technology may increase the complexity of business operation, thus triggering potential auditor changes.

Auditing standards define inherent risk as the likelihood of a potential misstatement in account balances without considering the effect of internal controls. The coefficient of *Inherent_Risk* captures inherent risk in inventory and accounts receivable and can be either positive or negative. Companies in the technology and software industries may have small inventories. Receivables resulting from pay-as-you-go pricing models are a function of volume of usage. The signs of these coefficients are not predicted. The $|DACC|$ coefficient can be positive because cloud companies are larger in size and are documented in literature to have higher incentives to manage earnings using discretionary accruals. Otherwise, we do not make a prediction on the coefficient of $|DACC|$.

The coefficient of *SEC404* is expected to be positive, as 91 percent of our sample has deployed cloud computing in the years 2008–2009, while 100 percent of these cloud companies became accelerated filers under Section 404 on internal controls in 2009 and 2010. The coefficients of *Restatement*, *ERRORD*, and *MWD* are related. When a company has material weaknesses in internal controls (*MWD*), a company is more likely to have related accounting errors (*ERRORD*) and may even restate its financial statements (*Restatements*) (Plumlee and Yohn 2010). Due to lack

[15] In our sample, 13 out of 67 post-cloud companies were involved in a merger and 5 out of 118 pre-cloud companies were involved in a merger. On the other hand, 20 non-cloud companies were involved in a merger.

of regulations on the cloud's internal controls, especially those related to security and privacy controls, cloud computing companies are more likely to have material weaknesses than non-cloud computing companies. This is likely to be associated with increased accounting errors and restatements. Singleton (2010) indicates that infrastructure costs are substantial; according to GAAP, these are treated as capital expenditures or operating expenses if the costs are outsourced. Revenue recognition can be complex, especially if multiple party arrangements are involved (Rashty and O'Shaughnessy 2010) and thus associated with more accounting errors. While R&D costs are expensed as incurred, software development costs may have complex accounting treatment depending on the stage of development and thus leading to increased accounting errors (or even restatements). Yet, accounting errors and restatements may not be necessarily related to cloud privacy and security issues.

About 59 percent of cloud firm-year obervations (109 out of 185 firm-year observations) have a *December* fiscal year-end; of the 67 cloud companies, 43 have a *December* fiscal year-end. The coefficient of *AudFees* is expected to be positive to accommodate for increased audit work, due to higher client business risk and more audit risk factors in cloud companies than in non-cloud companies. Similarly, longer audit report lags (*ARL*) indicate that the auditor needs more time to audit a client due to the client's business risks, complexity, and audit risks.

VI. FINDINGS

Descriptive Statistics

Table 3 provides the descriptive statistics of the pooled sample. Average total assets for companies in the sample are $6,104.2 million, and average audit fees and non-audit fees are $2,679,530.81 and $893,170.52, respectively. Average log of total assets is 5.78, with average liquidity position (*Liquidity*) at 7.03 percent of total assets. On average, companies in our sample are highly leveraged, with a 75.98 percent debt-to-equity ratio (*Leverage*). Average ROA is 35.33 percent, with 36.49 percent of the sample incurring a loss (*Loss*). In addition, average *Z-score* is 1.52. Altman (1968) indicates that a lower Z-score implies greater financial distress risk. Only 5.14 percent of the sample received a going concern opinion (*Going_Concern*), while 8.11 percent of the sample restated its financial statements (*Restatement*).

Average absolute discretionary accruals, $|DACC|$, is 0.71. Large absolute discretionary accruals are a measure of low earnings quality, consistent with Warfield et al. (1995). Big 4 auditors audited 70 percent of the companies in our sample, with tenure of less than three years (*Tenure*) in about 14.86 percent of the sample, and auditor change (*Audchange*) averaging 4.86 percent of the sample. Average inventory and accounts receivable to total assets (*Inherent_Risk*) is about 23.54 percent, which is expected because of the nature of the industries in which the cloud and control companies belong. About 87.30 percent of the companies in the sample are subject to Section 404 on internal controls over financial reporting (*SEC404*). About 4.05 percent of the companies in the sample had two or more material weaknesses in internal controls over financial reporting (*MWD*), with about 8.11 percent of the sample having one or more accounting errors due to the internal control issues (*ERRORD*).

Univariate Tests[16]

The univariate tests compare cloud computing companies with non-cloud computing companies, each with a subsample of 185 firm-year observations. Size, as measured by log of total assets, for

[16] For brevity, the univariate tests are not reported and are available upon request from the authors.

TABLE 3

Descriptive Statistics
(n = 370 Firm-Year Observations)

Variable	Mean	Std. Dev.	25th Percentile	Median	75th Percentile
Cloud_Tech	0.5	0.5	0	0.5	1
AT	6104.2	25399.78	93.53	309.91	1145.95
Audit_Fee	2679531	5565708	468000	1192710	2284690
Non_Audit_Fee	893170.5	4027617	6750	83271	377514
Size	5.7846	2.3341	4.5489	5.7395	7.0449
Liquidity	−0.0703	1.8486	0.0179	0.0992	0.1535
Leverage	0.7598	3.1738	0.2494	0.3836	0.5663
ROA	−0.3533	3.4381	−0.0229	0.0539	0.1005
Z-score	1.5237	34.8931	1.2915	2.9899	5.9074
Segment	2.0913	0.8498	1.6094	2.1972	2.6391
Loss	0.3649	0.4820	0	0	1
Merger	0.1027	0.3040	0	0	0
Litigation_Risk	0.7541	0.4312	1	1	1
AudFees	0.8641	0.1499	0.7718	0.9229	0.9889
NonaudFees	0.1359	0.1499	0.0111	0.0771	0.2282
Going_Concern	0.0514	0.2210	0	0	0
Audchange	0.0486	0.2154	0	0	0
Big4	0.7000	0.4589	0	1	1
Tenure	0.1486	0.3562	0	0	0
Inherent_Risk	0.2354	0.1958	0.1014	0.1598	0.3009
|DACC|	0.7079	2.8012	0.0094	0.0581	0.2233
Restatement	0.0811	0.2733	0	0	0
SEC404	0.8730	0.3335	1	1	1
ERRORD	0.0811	0.2733	0	0	0
MWD	0.0405	0.1975	0	0	0
ARL	4.0352	1.1657	3.9703	4.1589	4.3820
December	0.6270	0.4842	0	1	1

All variables are defined in Table 2.

cloud companies is higher than the control sample, but the difference is not statistically significant. We find that cloud companies have significantly higher leverage than non-cloud companies, with a p-value of 0.07, indicating that cloud companies are significantly more leveraged than non-cloud companies at less than a 10 percent level. Although not statistically significant, cloud companies are less liquid, less profitable, have less inventories and receivables, and have a larger number of segments and engage in fewer mergers than non-cloud companies. In addition, cloud companies have higher audit fees, longer ARL, are less likely to receive going concern opinions, are audited by Big 4 auditors, are more likely to be subject to Section 404, and have more material weaknesses, less accounting errors, and less financial restatements than non-cloud companies.

To obtain a closer insight of cloud companies, we compare pre- and post-cloud computing subsamples. The univariate test shows that after providing cloud technology, cloud companies become larger in size, less liquid, more leveraged, less profitable, less likely to receive going concern opinions, less likely to change auditors, have higher audit fees, longer auditor tenure, more material weaknesses, more accounting errors, and shorter ARL. These variables are not significant.

On the other hand, cloud companies have lower absolute discretionary accruals in a post-cloud period than in a pre-cloud period and are more likely to restate their financial statements. These results are significant at the 10 percent level. Lower discretionary accruals may be explained as deploying cloud computing, allowing for little investment in inventory and accounts receivable so traditional methods of earnings management are no longer available. Accounting errors may increase due to complexity and judgment involved when accounting for R&D, software, and hardware-related expenses and revenues.

Logistic Regression Results

In this section, results of the estimation of Model (1) are discussed.

Logistic Regression Comparing Cloud Companies with Non-Cloud Companies

Table 4 provides the estimation results of Equation (1).[17] Model (1) estimates Equation (1), where *Cloud_Tech* is 1 if a company is cloud provider, and 0 if a non-cloud company. Model (1) shows that the coefficient of *Leverage* is positive and significant at a p-value of 0.02, indicating that cloud companies are significantly more leveraged than non-cloud companies with a significance level of less than 5 percent. Moreover, cloud computing companies are more likely to have material weaknesses than non-cloud companies, as reflected in the significantly positive coefficient on *MWD* at a 1 percent level. Relating to *MWD*, the coefficient of *ERRORD* is negative and significant at the 1 percent level, indicating that cloud companies have lower accounting errors than non-cloud companies. These results are consistent with the univariate tests.

The coefficient of *Tenure* is negative and significant at a less than 1 percent level, indicating that cloud companies are more likely to have longer auditor tenure than non-cloud companies. Finally, *ARL* is positive and significant at the 1 percent level, indicating that cloud companies have longer audit delay, which is expected due to the increased IT complexities (Lin 2010). These results are consistent with univariate tests discussed earlier. All other variables are not statistically significant. The model's R^2 is 17.64 and model statistics are significant at the 1 percent level or less.

Logistic Regression Comparing Cloud Companies in Pre- and Post-Cloud Periods

Model (2) in Table 4 shows the estimation results of Equation (1), where the dependent variable is 1 if a cloud company is in a post-cloud period, and 0 if a cloud company is in a pre-cloud period. The results show that leverage is positive at the 10 percent level, suggesting that cloud companies are significantly more leveraged in the post-cloud period than in the pre-cloud period. In addition, segment is positive and significant at the 5 percent level.[18] Moreover, cloud companies are more likely to restate their financial statements after providing cloud technology compared to the pre-cloud period, with a p-value of 0.06. Other variables are not statistically significant. These results are reconcilable to the univariate tests. The model is significant at the less than 1 percent level as reflected in the Likelihood Ratio. Due to the small sample size and lack of sufficient variation in the independent variables, many of the variables are not statistically significant.

Summary of Findings

Results of the univariate tests and logistic regressions show that there are some differences between cloud and non-cloud companies, and between the pre- and post-cloud periods. These

[17] Results presented in the study are based on the scaled raw data. We elect not to Winsorize the data due to small sample size. However, if we Winsorize the data, we get the same results.

[18] However, this result conflicts with univariate tests but can be explained as a significant correlation between *Size* and *Segment* (correlation coefficient of 0.35 with p-value < 0.001).

TABLE 4

Logistic Regression

	Model (1)			Model (2)		
	***Cloud_Tech*: 1 if cloud company, and 0 otherwise**			***Cloud_Tech*: 1 if post-cloud period, and 0 if pre-cloud period**		
Dependent Variable	**Coeff.**	**Wald Chi-Squared**	**Pr. > Chi-Squared**	**Coeff.**	**Wald Chi-Squared**	**Pr. > Chi-Squared**
Intercept	−3.7457***	6.9028	0.0086	6.3642	0.8544	0.3553
Size	0.0875	1.1267	0.2885	0.2632	1.3632	0.2430
Liquidity	0.3090	0.2116	0.6455	−2.4825	0.3079	0.5790
Leverage	0.8838**	5.3737	0.0204	1.1230*	2.6907	0.1009
ROA	0.2213	1.7170	0.1901	1.3313	0.1710	0.6793
Z-score	0.0028	0.1667	0.6830	0.0008	0.0048	0.9447
Segment	0.0647	0.1122	0.7376	1.3454**	5.6019	0.0179
Loss	−0.1183	0.1601	0.6890	−1.3454	2.2207	0.1362
Merger	−0.0109	0.0007	0.9790	1.1348	0.5813	0.4458
Litigation_Risk	−0.1628	0.2978	0.5852	−0.1086	0.0150	0.9025
AudFees	1.0295	1.5130	0.2187	3.4039	1.6294	0.2018
Going_Concern	−0.9188	1.4136	0.2345	−2.3654	0.2975	0.5854
Big4	−0.0966	0.0833	0.7728	−0.1981	0.0386	0.8442
Tenure	−1.6231***	17.0044	< .0001	−2.1974	0.2889	0.5909
Inherent_Risk	−0.2450	0.1219	0.7269	−3.8733	1.6085	0.2047
|DACC|	0.0161	0.0884	0.7662	−0.1253	0.1170	0.7323
Restatement	−0.5983	1.7340	0.1879	2.3108**	4.0534	0.0441
SEC404	−0.1859	0.1828	0.6690	0.2835	0.0351	0.8513
ERRORD	−2.1188	7.9505	0.0048	−2.5459	2.4410	0.1182
MWD	2.5788***	6.5301	0.0106	0.8779	0.1370	0.7113
December	−0.1447	0.3301	0.5656	−0.8308	1.2669	0.2604
ARL	0.6775***	16.1311	< .0001	1.0348	0.6752	0.4112
Year Indicators		Included			Included	
n	370			185		
R^2	0.1757			0.5687		
Likelihood Ratio Chi-squared (Pr. > Chi)	70.9175 (< 0.0001)			155.5769 (< 0.0001)		
Score Chi-squared (Pr. > Chi)	54.0286 (0.0004)			120.5837 (< 0.0001)		
Wald Chi-squared (Pr. > Chi)	43.4599 (0.0088)			43.6493 (0.0738)		

*, **, *** Indicate significance at 10 percent, 5 percent, and 1 percent respectively.
All variables are defined in Table 2.

results show that cloud companies are more leveraged and more likely to have two or more material weaknesses in the internal controls, and have longer audit tenure and longer ARL when compared to non-cloud companies. Cloud companies are more likely to restate their financial statements in the post-cloud period compared to the pre-cloud period. However, several variables are not significant. Two explanations are offered: (1) cloud technology is an emerging technology that is complex, and

it exposes businesses to risks not captured by risk variables used in the study; and (2) the sample size is small and lack of variation in certain variables may be driving the results.

VII. CONCLUSIONS AND FUTURE RESEARCH

Conclusions

In the first part of this study, we provide an overview of cloud computing, its evolution, benefits, and challenges. We also discuss the emerging standards that are being developed to address the opportunities and challenges of cloud technology (e.g., NIST, SAS 70, and COSO Framework). This overview shows that as a result of changes in the business environment, globalization, and technological advancements, companies have adopted innovative business models, restructured their day-to-day operations, and relied greatly on IT outsourcing. Cloud computing has evolved from generations of mainframes, client-server architecture, ASPs, and SaaS. With the benefits and capabilities that cloud computing provide, businesses become more complex, and multiple risks arise. These risks are being addressed by formally defining cloud computing, building a roadmap to cloud standards, and providing guidance on how to manage and audit this technology. Our literature review on the effects of IT and IT outsourcing on audits shows that auditors respond to cloud technology for compliance and assurance purposes (e.g., Davis et al. 2006; Singleton 2010; Ames and Brown 2011; Curtis et al. 2009). As such, we expect that emergence of cloud computing places an increased burden on auditors.

In the second part of the study, we use a sample of hand-collected data on cloud computing to empirically examine risk characteristics. We identify risk characteristics based on prior research in accounting and auditing literature to capture clients' risks and audit risks. We find that only for certain risk variables are cloud providers riskier than non-cloud companies. These results may indicate that the risks/challenges discussed in Sections II and III are not captured by our measures of cloud risk constructs or are measured inaccurately. Cloud providers have innovative business models, so using variables that capture risks in "traditional" business models may not be appropriate.

Future Research

The empirical results documented in this study are significant because these results show that research is needed in this area. Follow-up research on our study and studies by Knolmayer and Asprion (2011) and ISACA (2009b, 2010) is desirable. Future areas of research are proposed:

- Future research may use alternative research methods such as surveys, interviews, and field studies to capture how the conduct of an audit is affected by cloud computing and how auditors assess risks in practice. Determining the scope of audit, assessing the risk of material misstatements, and evaluating the effect of internal controls on the financial statements—all require investigation as to how auditors comply with regulatory requirements in cloud settings. Such research methods may provide a wealth of knowledge about risk assessment and risk management and allow for better measurement of risk constructs.
- Although arguments can be made that IT may provide a ripe opportunity for fraud (Grabski et al. 2011), auditors must be cautious that fraud can take place even by simple means. Future studies may use audit engagement data to examine whether cloud providers and cloud users are more likely to have material misstatements in their financial statements, and what the nature and extent of these misstatements are. In addition, mapping cloud risks to misstatements in the financial statements would guide in risk management and internal controls practices to prevent or detect misstatements in the financial statements in a timely manner.

- Regulatory standards are adaptive to emerging business models and evolving technologies, and auditors develop tools and techniques to efficiently and effectively conduct audits. Therefore, auditing cloud computing will see advances in audit tools and techniques. Future studies may explore applicability and efficiency of using continuous auditing, especially for higher-risk clouds (e.g., public clouds). Examining security in real time throughout the year will have implications for the financial statement audit by reducing end-of-year audit procedures. In recent years, we have seen multiple continuous audit architecture proposed in ERP systems (e.g., Embedded Audit Module [EAM] by Groomer and Murthy [1989]; Monitoring and Control Layer [MCL] by Vasarhelyi et al. [2004]; Ghosting EAM by Kuhn and Sutton [2010]). Research may investigate the feasibility of imposing continuous audit architecture on cloud providers' data storage clouds.
- Future research may also investigate cloud service models (IaaS, PaaS, and SaaS) and deployment models (public, private, community, hybrid) by using simulation models. Simulation models will not only allow us to understand risks, but how to manage risks effectively.
- Future studies may address the role of corporate governance in outsourcing IT and best practices for companies to sustain regulatory-compliant status. Both corporate governance and risk management have come under regulatory scrutiny in recent years.
- Future research may investigate what governance and risk management practices may work and what may not in a cloud environment.

REFERENCES

ACL. 2010. *ACL Products for Technology Assurance*. Vancouver, BC: ACL.

Ahn, J. G., C. S. Leem, and J. H. Yang. 2001. A framework for certification and audit of application service providers—ASP. *Journal of Systems Integration* 10 (239): 239–252.

Alles, M., G. Brennan, A. Kogan, and M. A. Vasarhelyi. 2006. Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems* 7 (2): 137–161.

Altman, E. 1968. Financial ratios, discriminant analysis, and the prediction of corporation bankruptcy. *Journal of Finance* 23: 589–609.

American Institute of Certified Public Accountants (AICPA). 1992. *Service Organizations*. SAS 70. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2001. *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*. SAS 94. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2011. *Reporting on Controls at a Service Organization*. SSAE 16. New York, NY: AICPA.

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

Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, and A. Konwinski. 2010. A view of cloud computing. *Communications of the ACM* 53 (4): 50–58.

Billing, K. 2001. Risk e-business. *Accountancy* 27 (1294): 124–125.

Blaskovich, J., and N. Mintchik. 2011. Information technology outsourcing: A taxonomy of prior studies and direction for future research. *Journal of Information Systems* 25 (1): 1–36.

Buyya, R., C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. 2009. Cloud computing and IT emerging platforms: Vision, hype, and reality for delivery computing as the 5th utility. *Future Generation Computer Systems* 25: 599–616.

Cannon, J. C. 2004. *Privacy: What Developers and IT Professionals Should Know*. Boston, MA: Addison-Wesley.

Cash, J. I., A. D. Bailey Jr., and B. Andrew. 1977. A survey of techniques for auditing EDP-based accounting information systems. *The Accounting Review* 22 (4): 813–832.

Chou, C., and J. Chang. 2010. Continuous auditing for web-released financial information. *Review of Accounting and Finance* 9 (1): 4–32.

Cohen, R. 2009. Examining cloud computing mergers and acquisitions. Available at: http://java.sys-con.com/node/893141

Committee of Sponsoring Organizations of Treadway Commission (COSO). 2011. *Internal Control—Integrated Framework*. Exposure draft. New York, NY: COSO.

Curtis, M. B., J. G. Jenkins, J. C. Bedard, and D. R. Deis. 2009. Auditors' training and proficiency in information systems: A research synthesis. *Journal of Information Systems* 23 (1): 79–96.

Davis, C., M. Schiller, and K. Wheeler. 2006. *IT Auditing: Using Controls to Protect Information Assets: Auditing Cloud Computing and Outsourced Operations*. New York, NY: McGraw-Hill Osborne Media.

Debreceny, R. S., G. L. Gray, J. Ng, and K. Lee. 2005. Embedded audit modules in enterprise resource planning systems: Implementation and functionality. *Journal of Information Systems* 19 (2): 7–27.

DeFelice, A. 2010. Cloud computing: What accountants need to know. *Journal of Accountancy* (October): 50–55.

Deshmukh, A. 2006. *Digital Accounting: The Effects of the Internet and ERP on Accounting*. Hershey, PA: IRM Press.

Du, H., and Y. Gong. 2010. Cloud computing, accounting, auditing, and beyond. *The CPA Journal* (October): 66–70.

Elder, R., Y. Zhang, J. Zhou, and N. Zhou. 2009. Internal control weakness and client risk management. *Journal of Accounting, Auditing and Finance* 24 (4): 543–579.

Francis, J. D., D. Philbrick, and K. Schipper. 1994. Shareholder litigation and corporation disclosures. *Journal of Accounting Research* 32: 137–164.

Garland, P., R. Gittings, and M. Pearl. 2010. Cloud computing gets strategic: Reducing technology costs is just the starting point. *PricewaterhouseCoopers View* 13: 1–12.

Gartner Research. 2011. Gartner identifies seven major projects CIOs should consider during the next three years. Press Release. Available at: http://www.gartner.com/it/page.jsp?id=1465614

Gill, R. 2011. Why cloud computing matters to finance. *Strategic Finance* (January): 43–47.

Glover, S., S. Liddle, and D. Prawitt D. 2001. *E-Business: Principles and Strategies for Accountants*. Englewood Cliffs, NJ: Prentice Hall.

Grabski, S. V., S. A. Leech, and P. J. Schmidt. 2011. A review of ERP research: A future agenda for accounting information systems. *Journal of Information Systems* 25 (1): 37–78.

Groomer, S. M., and U. S. Murthy. 1989. Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems* 3 (2): 53–69.

Harauz, J., L. M. Kaufman, and B. Potter. 2009. Data security in the world of cloud computing. *IEEE Security & Privacy* 7 (4): 61–64.

Hogan, M. D., F. Liu, A. W. Sokol, and T. Jin. 2011. *NIST Cloud Computing Standards Roadmap*. Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024

Information Commissioner's Office. 2008. Data Protection guidance note: Privacy enhancing technologies (PETs). Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies_v2.pdf

Information Systems Audit and Control Association (ISACA). 2009a. *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives*. Rolling Meadows, IL: ISACA.

Information Systems Audit and Control Association (ISACA). 2009b. *Cloud Computing Management Audit/Assurance Program*. Rolling Meadows, IL: ISACA.

Information Systems Audit and Control Association (ISACA). 2010. *Cloud Computing Management Audit/Assurance Program*. Rolling Meadows, IL: ISACA.

IT Governance Institute (ITGI). 2005. *COBIT 4.0: Control Objectives for Information and Related Technology*. Rolling Meadows, IL: ITGI.

Jansen, W., and T. Grance. 2011. *Guidelines on Security and Privacy in Public Cloud Computing*. NIST Special Publication 800-144. Gaithersburg, MD: NIST.

Janvrin, J. D., J. Bierstaker, and D. J. Lowe. 2008. An examination of audit information technology use and perceived importance. *Accounting Horizons* 22 (1): 1–21.

Johnstone, K. 2000. Client-acceptance decisions: Simultaneous effects of client business risk, audit risk, auditor business risk, and risk adaption. *Auditing: A Journal of Practice & Theory* 19 (1): 1–25.

Kilpatrick, T. 2000. Auditing manufacturing costs. *The Internal Auditor* 57 (3): 25.

Knolmayer, F., and P. Asprion. 2011. *Assuring Compliance in IT Subcontracting and Cloud Computing*. Working paper, University of Bern.

Kotb, A., and C. Roberts. 2011. The impact of e-business on the audit process: An investigation of the factors leading to change. *International Journal of Auditing* 15: 150–175.

Kothari, S., A., Leone, and C. Wasley. 2005. Performance matched discretionary accrual measures. *Journal of Accounting and Economics* 39 (1): 163–197.

KPMG. 2010. Audit in the cloud: Security audits versus cloud computing. Available at: http://www.slideshare.net/eburon/audit-in-the-cloud-kpmg

Kuhn J. R., Jr., and S. G. Sutton. 2010. Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems* 24 (1): 91–112.

Liang, D., F. Lin, and S. Wu. 2001. Electronically auditing EDP systems with the support of emerging information technologies. *International Journal of Accounting Information Systems* 2 (2): 130–147.

Licklider, J. C. R. 1963. *Memorandum for: Members and Affiliates of the Intergalactic Computer Network; Topics for Discussion at the Forthcoming Meeting*. Washington, D.C.: Advanced Research Projects Agency.

Lin, P. P. 2010. SaaS: What accountants need to know. *The CPA Journal* 40 (6): 68–72.

McCarthy, J. 1961. Centennial Keynote Address. Massachusetts Institute of Technology.

Moeller, R. 2010. *IT Audit, Control and Security*. Hoboken, NJ: John Wiley & Sons.

Mohamed, A. 2009. A history of cloud computing. Available at: http://www.computerweekly.com/Articles/2009/06/10/235429/A-history-of-cloud-computing.htm

Moltzen, E. F. 2010. Analysis: Cloud stocks flying higher and higher. Available at: http://www.crn.com/news/channel-programs/222300414/analysis-cloud-stocks-flying-higher-and-higher.htm;jsessionid=LRLqmGqyEBtVG7A00Z7bpw**.ecappj01

National Institute of Standards and Technology (NIST). 2012. Inventory of standards relevant to cloud computing. Available at: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory

Pathak, J., and M. Lind. 2010. An e-business audit service model in the B2B context. *Information Systems Management* 27 (2): 146–155.

Public Company Accounting Oversight Board (PCAOB). 2007. *An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements*. Auditing Standard No. 5, Release No. 2007-005A. Washington, DC: PCAOB.

Pearson, S. 2009. *Taking Account of Privacy when Designing Cloud Computing Services*. Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, BC.

Plumlee, M., and T. L. Yohn. 2010. An analysis of the underlying causes attributed to restatements. *Accounting Horizons* 24 (41).

Rashty, J., and J. O'Shaughnessy. 2010. Revenue recognition for cloud-based computing arrangements. *The CPA Journal* (November): 32–35.

Rezaee, Z., R. Elam, and A. Sharbatoghlie. 2001. Continuous auditing: The audit of the future. *Managerial Auditing Journal* 16 (3): 150–158.

Ross, S. J. 2010. Recovery in the cloud. *Information Systems Control Journal* 3: 4–5.

Shroff, G. 2010. *Enterprise Cloud Computing: Technology, Architecture, Application*. New York, NY: Cambridge University Press.

Singleton, T. W. 2010. IT audits of cloud and SaaS. *ISACA Journal* (3): 1–3.

Sutton, S. G. 2006. Extended-enterprise systems' impact on enterprise risk management. *Journal of Enterprise Information Management* 19 (1/ 2): 97–114.

Sutton, S. G., and C. Hampton. 2003. Risk assessment in an extended enterprise environment: Redefining the audit model. *International Journal of Accounting Information Systems* 4 (4): 57–73.

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

Vael, M. 2010. Cloud computing: An insight in the governance and security aspects. Available at: http://www.isaca.org/Groups/Professional-English/information-secuirty-management/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

Vasarhelyi, M. A., M. Alles, and A. Kogan. 2004. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting* 1: 1–21.

Warfield, T. D., J. J. Wild, and K. L. Wild. 1995. Managerial ownership, accounting choices, and informativeness of earnings. *Journal of Accounting and Economics* 20: 61–91.

Westervelt, R. 2006. New SAP business unit to focus on compliance. Available at: http://searchsap.techtarget.com/news/1188877/New-SAP-business-unit-to-focus-on-compliance

Wright, S., and A. M. Wright. 2002. Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* 16 (1, Supplement): 99–113.

Zhao, N., D. C. Yen, and I. C. Chang. 2004. Auditing in the e-commerce era. *Information Management and Computer Security* 12 (5): 389–400.