JOURNAL OF INFORMATION SYSTEMS
Vol. 30, No. 3
Fall 2016
pp. 173–189

American Accounting Association
DOI: 10.2308/isys-51494

COMMENTARY

Business in the Cloud: Research Questions on Governance, Audit, and Assurance

Pamela J. Schmidt
Washburn University

Jason T. Wood
PricewaterhouseCoopers

Severin V. Grabski
Michigan State University

ABSTRACT: Cloud computing services are finding rapid adoption as organizations seek cost reduction, technical expertise, flexibility, and adaptable mechanisms to attain advantages in fast-moving business environments. The related considerations of governance, audit, and assurance of cloud computing services might be inadvertently overlooked in a rush to adopt these cloud services. This paper focuses on cloud computing governance and audit issues by presenting research questions informed by both practice and research. A cloud computing ecosystem is presented and an IT Governance framework (Wilkin and Chenhall 2010) is referenced as a means to structure research questions. Key issues of risk, security, monitoring, control, and compliance should be considered early in the cloud services decision process. The tight coupling of intercompany operations between the cloud client and cloud provider(s) forms an interdependent, operationally coupled ecosystem. Planned governance is needed to achieve a well-governed, functional, and secure cloud computing environment. The audit role is complicated when the organization's financial data and/or critical applications are hosted externally with a cloud service provider that may use other cloud service providers.

Keywords: IT governance; IT audit; cloud computing; risk assessment; emerging technology; research questions.

I. INTRODUCTION

This paper offers a set of key research questions related to governance, audit, and assurance of external cloud computing services. Emphasis is placed on areas where the emergence of cloud computing services requires the attention of board and executive levels, and where cloud computing decisions can result in the need for additional (or modified) governance and audit activities. This cloud research discussion is organized around the perspectives of cooperating parties involved in the cloud computing ecosystem.[1] Included in a cloud computing ecosystem are the (1) cloud service users (CSUs) as contracting clients of cloud computing, (2) the cloud service providers (CSPs) of the cloud computing software services

The authors thank the panel participants at the 2015 Accounting Information Systems (ASYS) Special Interest Group (SIG) Pre-ICIS Conference in Auckland, New Zealand, particularly Anthony Steele, CA, and Roger Debreceny, Ph.D., for inspiring and informing this paper. Professor Schmidt gratefully acknowledges the financial support of a 2014 Beatrice Summer Research Chair Grant from Washburn University.

Supplemental material can be accessed by clicking the link in Appendix A.

Editor's note: Accepted by Roger S. Debreceny.

Submitted: May 2015
Accepted: April 2016
Published Online: June 2016

[1] Supplemental material is available by using the link provided in Appendix A. The supplement provides the cloud research questions organized and cross-referenced with the IT Governance framework (Wilkin and Chenhall 2010).

(e.g., Software as a Service known as SaaS) that may have contracted with other "nested" CSPs for services (e.g., Platform as a Service, known as PaaS, and Infrastructure as a Service, known as IaaS), (3) the cloud service partner (CSN) to the cloud service providers (CSNs may provide content, application development, or other specialized services), and (4) the external auditors of the cloud computing services. The external auditor role includes the auditors of the CSU and the external auditors of the CSP that offer cloud services to clients. A cloud service audit may be part of the external audit of the CSU or it may be performed on behalf of the CSP. The primary focus of this paper is on the perspectives of governance and assurance parties, namely boards of directors, executives, and external auditors (both of the CSU and the audit reporting related to the CSP). A key differentiator of this cloud computing ecosystem from prior IT services relationships is the acknowledgement of shared risk management responsibilities.[2] Further, this paper suggests a proactive governance approach, with the board and executives consulting early on the cloud computing service options with their own technology advisory committee and external auditors.

IT governance and, hence, cloud computing governance, needs to be an integral part of corporate governance. A long-standing tenet of IT governance has been allocation of decision rights. In early discussions of IT governance, Weill and Ross (2004, 8) stated the importance of "specifying the decision rights and accountability to encourage desirable behavior in the use of IT." A key part of IT governance is to establish processes and clearly assign authority for providing information about IT and making IT decisions. This perspective has been extended by the Information Technology Governance Institute (ITGI) and ISACA that state, "Enterprise [corporate] governance is a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly" (ITGI 2003, 6). They also observe that "Boards and executive management need to extend governance to IT and provide the leadership, organisational structures and processes that ensure that the enterprise's IT *sustains and extends the enterprise's strategies and objectives*" (ITGI 2003; emphasis in the original).

The research questions presented in Section III are organized by activities and responsibilities in the cloud ecosystem. These same research questions are then cross-referenced to a leading taxonomy for IT Governance (Wilkin and Chenhall 2010) in a downloadable supplement to this paper titled "A Supplement to Business in the Cloud: Research Questions on Governance, Audit and Assurance," which is available using the link in Appendix A. This framework is organized into five key areas: Strategic Alignment (SA), Risk Management (RK), and Resource Management (RM), along with outcome areas of Value Delivery (VD) and Performance Measurement (PM). This IT Governance taxonomy highlights the critical role of the board in leading the assessment of the strategic alignment of cloud computing services, while concurrently giving guidance regarding risk management. The cross-boundary nature of cloud computing inherently reduces observability and control by the contracting client organization. Cloud computing services require expanding governance such as considering the degree of interdependence, shared management and control, disaster recovery, vendor lock-in, and a host of other governance issues, all complicating corporate governance and assurance.

Some organizations are leveraging cloud services for IT flexibility and agility, seeking cloud computing as the basis for sustained competitive advantage (Stamas, Kaarst-Brown, and Bernard 2014). Other organizations have begun to view IT as a utility (Buyya, Yeo, Venugogal, Broberg, and Brandic 2009) rather than as an economic resource or competitive advantage. Yet, there is a risk that the rapid adoption of cloud-based services may be over reaching the ability of corporations and their auditors to manage the risks and complexities that are inherent in cloud-based environments. Internal functional departments or the IT organization may have directly contracted for some cloud-based services without a review at appropriately high levels of governance. A company reported that employees were using nearly 900 cloud-based services, yet only 20 of these services were authorized for use (Mont 2015). Truong and Dustdar (2011, 76) report that in cloud computing service offerings "cost estimation and monitoring tools are not well supported, platform and programming support for CSE (computational science and engineering) in cloud systems are poor, and generic CSE services have not been widely deployed in the cloud under the SaaS model." Business activities traditionally and routinely handled at the tactical or operational level, such as vetting service vendors and signing IT outsourcing contracts, may continue to occur with cloud computing arrangements. A change to internal policies and past procedures are needed to ensure that sufficient attention is paid to the cloud corporate governance implications.

It is advisable that any consideration of shared external (public or hybrid) cloud computing services should trigger a fundamental review and expansion of corporate governance policies. Such a review should consider the full extent of interdependencies on external cloud providers. Shareholders, customers, and suppliers will be concerned over privacy and cyber-security in cloud computing services that are contracted for by the organization. As such, the board should develop a holistic governance approach before a cloud service provider is engaged. Effectively, the client organization is handing over

[2] For example, Amazon Web Services (AWS) acknowledges the emergence of "shared governance" responsibilities between the Cloud Service User and Cloud Service Provider (Amazon.com 2015).

management and control of their corporate data and IT services. The board would be abdicating its responsibilities if it allowed the cloud provider to dictate IT governance and assurance responsibilities.

To convey a broad corporate governance point of view, this paper takes the perspective that engaging an external cloud computing service draws the contracting enterprise into a tightly knit "cloud computing ecosystem" (Iyer and Henderson 2010; Briscoe and Marinos 2009). While prior research on the cloud computing ecosystem focused on the technical and user community, the research questions presented here emphasize the strategy, risk, and control issues inherent in this ecosystem. The cloud ecosystem is notable for its potential (1) for a high degree of interdependency of strategy, risk management, and assurance, (2) new boundary-spanning operational processes and IT coordination activities, and (3) for the possibility of multiple layers of cloud services with dependency upon other external IT infrastructure entities. This existence of arms-length, separate company IT infrastructures may inhibit direct monitoring, constrain full disclosure, obscure dependencies, and reduce the cloud client's control over its critical IT infrastructure. As illustrated in the "Trusted Cloud Reference Architecture from the Cloud Security Alliance" (ISACA 2014), a cloud service offering may take the form of a private, hybrid, or public cloud (the latter two supporting multiple CSU tenants) and can include multiple layers of CSPs such as SaaS, PaaS, and IaaS individually or in collaboration. Each layered provider can independently decide when it performs updates and maintenance, perhaps with minimal notification to service users. Multiple layers of cloud services also likely lead to reliance on multiple audit reports (an audit report on the contracting enterprise and a separate report on the cloud service provider). There are multiple stakeholders looking at CSP audit reports including the contracting CSU itself, along with its end customers, trading partners, and investors.

A holistic perspective and consolidated oversight of cloud services should occur (Fortis and Munteanu 2014). Each party has its own particular role and perspective, and all are essential to (or depend upon) achieving a functional, secure, and well-governed cloud computing environment. It is particularly worthwhile to consider the contracting enterprise's board of directors' role and the external auditor's role as providing beneficial lenses through which to view the cloud computing relationships.

The cloud computing infrastructure has been often defined from a technology perspective in a number of standards publications and technical architecture papers (Liu et al. 2011; Mahmood 2014; Mell and Grance 2011; Ritteninghouse and Ransome 2010). From a technology evolution perspective, cloud computing is based on number of building block technologies consolidated into flexible, metered commodity IT services. These building block technologies include pervasive broadband networking, dynamic processor allocation, service-oriented architecture, enterprise systems, and mature virtualization capabilities. Swift allocation and reallocation of virtualized IT capacity has set the stage for cloud services to provide client companies with IT as an expense without large capital outlays to prepare for future capacity needs (Buyya et al. 2009).

Notably, cloud computing has many architectural variations. Implementations by cloud service providers vary widely and their detailed layout may not be well publicized. Forms of cloud services range from single-CSU private clouds to multiple tenant-style hybrid or public clouds (with several cloud client companies utilizing one shared IT infrastructure). Based on considering strategic alignment, risk, and resource management, boards need to strategically decide whether they should use private clouds, public clouds, or some combination of private and public clouds to meet their overall business goals. Cloud services are offered in several models. For example, an SaaS may be layered if the SaaS provider contracts out to another PaaS provider or IaaS provider. Some CSU contract for enterprise support services and rely on a wholly external cloud-based Enterprise Resource Planning (ERP) system (Grabski, Leech, and Schmidt 2011), which results in a full range of financial and operation functionality hosted by the CSP, entirely external to the CSU. Boards should carefully assess cloud options using guidelines such as the IT Governance framework (Wilkin and Chenhall 2010), the Cloud Security Alliance's Cloud Controls Matrix (Cloud Security Alliance 2015), and the Cloud Capability Maturity Model (Grabski and Schmidt 2014). Foremost, it is critical for the board of directors and executives to be apprised of the level of risk associated with the adopted approach. Existing governance mechanisms need to be reviewed and enhanced to ensure that appropriate levels of risk assessment, on-going oversight, assurance, and compliance are established before embarking on a contracted cloud outsourcing arrangement. As cloud providers themselves may rely on other cloud services as another layer of hidden infrastructure, the full extent of the external, layered cloud-based IT infrastructure should be reviewed and assessed with a corporate governance mindset.

The rest of this paper is organized as follows. The "Cloud Ecosystem" section presents a governance-based perspective in describing the structure of the cloud ecosystem (Sotomayor, Montero, Llorente, and Foster 2009) that illuminates the need for "chains of accountability" (Pearson 2011). It identifies key participating parties and describes their role within the cloud ecosystem. As Pearson (2011, 67) explains:

> In the cloud, it will be harder to establish the risks and obligations, implement appropriate operational responses and deal with regulatory requirements. The notions of transparency and assurance come in more strongly and it is necessary to ensure "chains of accountability." So, the communities responsible for data stewardship (who are typically organisational IT security, legal, operations and compliance staff) place responsibilities/constraints on other individuals or on the way systems operate, and these constraints are met along the chain of provision.

Section III presents cloud computing research questions that address shared governance and cloud auditing. It is organized by activities and areas of responsibility including the seven areas of strategy, contracting, operations, audit, total cost of cloud computing ownership (TCCO), critical success factors (CSF), and stakeholders' concerns. When research questions are listed in the text, each is followed by a parenthetical expression with the abbreviated indicator for its related subtopic within the Wilkin and Chenhall (2010) IT Governance framework. For example, a tag of (SA2) is referencing the Strategic Alignment area and a specific subarea, No. 2, by number. A downloadable supplement is available online titled "A Supplement to Business in the Cloud: Research Questions on Cloud Governance, Audit, and Assurance," which is organized by these subareas defined in the Wilkin and Chenhall (2010) IT Governance framework. This supplement, accessible using the link in Appendix A, contains a full list of this paper's cloud governance research questions providing a cross-reference between the research questions and topics in the IT Governance framework. There, each cloud research question is preceded by the topic heading under which it appears within the seven areas of strategy, contracting, operations, audit, TCCO, CSF, and stakeholders concerns. Section IV provides some concluding thoughts.

II. CLOUD ECOSYSTEM

As previously identified, the cloud computing ecosystem includes the:

a. Cloud Service User (CSU): organizations contracting to use external cloud computing services.
b. Cloud Service Provider (CSP): provider(s) of the cloud services that include software services and also the cloud computing hardware and infrastructure services that are used in the delivery and storage of data and applications (which may include multiple companies unknown to the primary contractor of a software service).
c. Cloud Service Partners (CSN): partners of the cloud service providers that provide content, application development, or other services (International Telecommunication Union [ITU-T] 2012).
d. Auditors: external auditors of the CSU and potentially those of the CSP.
e. Stakeholders: various parties that rely on the external auditor's report.

The external audit of the CSP could be contracted by the CSP itself, but the CSU might also need an audit performed by their external auditor if the CSP contracted audit did not meet the needs of the CSU's auditor. Others also concerned by IT supported by a cloud ecosystem are customers, trading partners, and investors in the organization contracting cloud services. These parties want to be assured that data and computing resources are properly protected, controlled, and utilized.

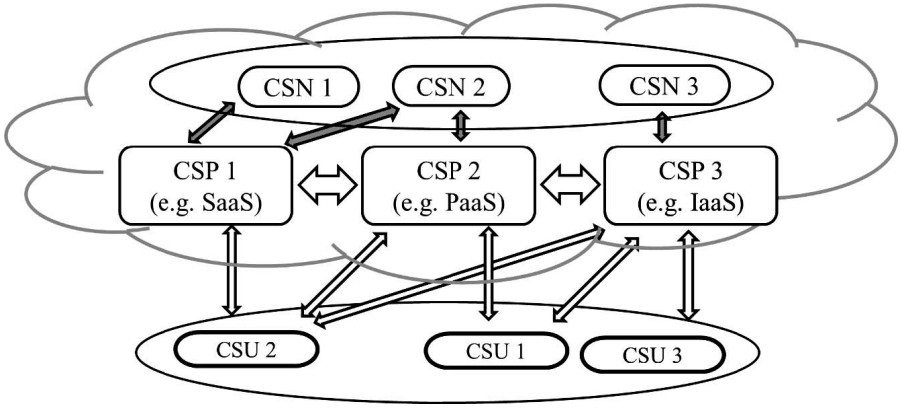
Ultimate corporate governance responsibility lies with the board of directors and executives of the CSU. Corporate governance strives to manage the firm's operations to "effectively meet shareholder expectations for financial and environmental prudence, reputation, competitive edge, and risk management" (Wilkin and Chenhall 2010, 108). This means that the CSU, not the cloud provider, should define the cloud governance ecosystem across the entire scope of the firm's IT support environment.

Three views of the cloud ecosystem (Figures 1, 2, and 3) are presented. Figure 1 presents only the basic parties involved in cloud computing. This view of the cloud ecosystem focuses on the CSU, CSP, and CSN entities and is taken from the ITU-T (2012) report. It does not consider any governance factors, nor does it consider any trading partners or customers of the CSU.

Figure 2 expands upon Figure 1 to consider CSU1 to be the organization of interest that is contracting for the cloud service. The other parties presented in Figure 2 include (1) CSU1's audit firm; (2) CSP1, the primary contracted cloud service provider with possible relations to other cloud providers, e.g., CSP2 and CSP3 (as layers of a complete cloud computing service offering); (3) the shareholders (and potential shareholders) of CSU1; (4) the customer base of the organization; and (5) the trading partners of CSU1. Some of these parties are identified in key standards documents such as the National Institute of Standards and Technology (NIST) Definition of Cloud Computing (Mell and Grance 2011) and the NIST Cloud Computing Reference Architecture (Liu et al. 2011). Figure 2 assumes that the very simple case of CSU1 to CSP1 as the only service relationship that was reviewed by the board of directors and is officially contracted by the organization. Figure 2 also includes other ungoverned or "shadow cloud" relationships depicted between CSU1 with CSP2 and CSP3 (directly contracted individuals or department managers without formal governance approval). These "shadow cloud systems" increase the risk to the organization (Vijayan 2014) and are represented by the "X" over the relationship lines from CSU1 to CSP2 and CSP3. The role of the external auditor is also made explicit; their audit report on CSU1 can be used by investors, customers, and trading partners (as these parties determine whether to invest in, or do business with CSU1). As part of the annual financial statement audit report, the external auditor needs to be able to specify the reliance on CSP1 with respect to material financial statement information and may either audit the IT security and controls of CSP1 or request an SOC (Service Organization Controls)[3] control assurance report from CSP1 detailing this information (this is noted

[3] For background information about Service Organization Controls (SOC) reports see "FAQs—New Service Organization Standards and Implementation Guidance" at: http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/FAQs_Service_Orgs.pdf.

FIGURE 1
Three Actors of a Cloud Ecosystem



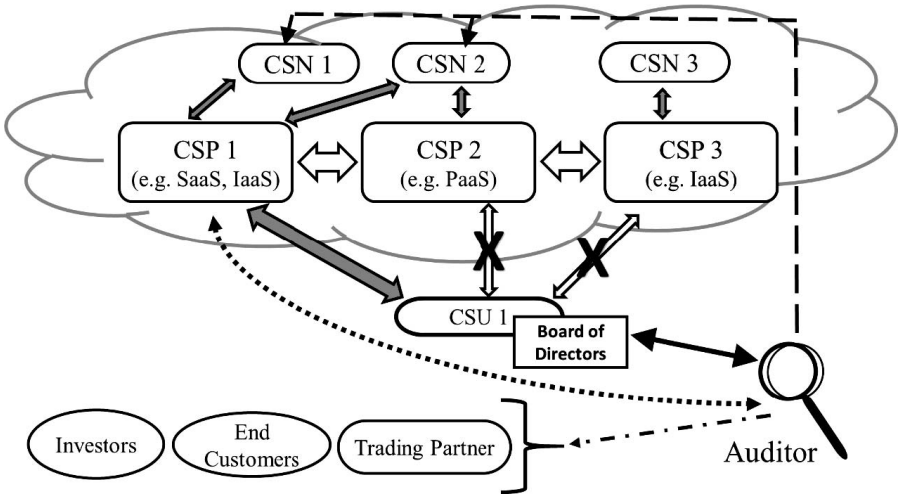
Source: ITU-T (2012).

CSN = Cloud Service Partner. The entity that provides contracted services to the CSP, such as content, application development, or other services.

CSP = Cloud Service Provider. The entity that provides a cloud computing service (e.g., SaaS, IaaS, PaaS). The CSP may rely on other CSPs to provide additional needed services (represented by the arrows between CSPs in the diagram).

CSU = Cloud Service User. The entity that contracts for the use of a cloud computing service. A CSU might be using multiple cloud services as indicated by the arrows between the CSU and CSP.

FIGURE 2
Cloud Computing Ecosystem
CSU 1 with Formal Governance Structure



Adapted from ITU-T (2012).

(___) The solid line between the CSU BoD (Board of Directors) and Auditor represents the formal audit relationship.

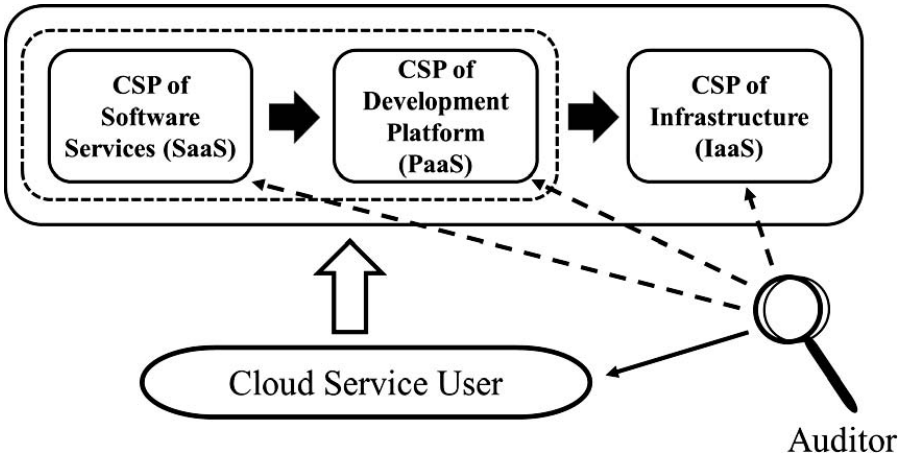
(. . . .) The dotted line between Auditor and CSP represents the auditor either performing an audit of the CSP as specified in the auditing standards (or basing their opinion on that CSP's corresponding auditor's audit report).

(_ _ _) The long dashed lines between Auditor and CSNs represent a potential audit of those entities (or basing of an audit opinion on that company's corresponding auditor's report).

(– · – · – · –) The dot-dashed lines between Auditor and End Customer, Trading Partner, and Investor represent the potential use of the audit report by these entities.

(X) The X'ed lines between the CSU and CSPs represent employee and departmental use of cloud services that have not been formally approved by the organization. The risk is that these "shadow cloud" services might not be discovered during the course of a financial audit.

FIGURE 3
Audit Involving Nested Layers of Cloud Computing Services



Based on cloud services as described in ISACA (2014).

External auditor engagement with a cloud service user (company) that is contracting with a SaaS cloud service provider (that may use PaaS and/or IaaS services from other providers).

(- - - -) The dotted line between Auditor and CSPs represents the auditor either performing an audit of the CSP as specified in the auditing standards (or basing their audit opinion on a corresponding CSP auditor's audit report).

(_____) The solid line between Cloud Service User and Auditor represents the primary audit relationship.

Broad, black arrows represent cloud computing contracts between cloud computing providers.

as a dotted line between CSP1 and the auditor). CSP1's auditor will likely need to request an SOC control assurance report from CSP2, and possibly CSP3 (denoted with the long dashed line in the figure), in order to provide the complete financial audit report needed by CSU1's auditors. Additionally, the auditor may need to gain SOC control assurances from CSN2 and CSN3 (noted by the long dashed lines).

Distinct from the governed cloud provider relationship, other specialized CSPs (e.g., for customer relationship management, file sharing) may have been directly contracted by specific business units. The "shadow cloud service" providers, e.g., Figure 2: CSP2 and CSP3, will likely not be contacted for an SOC control assurance report unless the use of these "shadow cloud services" are detected in the financial audit. If these "shadow cloud services" are not formally acknowledged and approved, then the board, the auditors, and the IT department may not have the opportunity to assess potential risk exposures. If these CSPs are used only for file storage or for other nonfinancial purposes, e.g., application development, then there is a high probability that they will not be discovered. With these issues in mind, the cloud ecosystem in Figure 2 highlights the role of the board of directors in establishing formalized governance related to cloud computing. Figure 2 also highlights the role of the auditor in providing assertions that the appropriate governance policies and procedures are followed.

If CSP1 is a software service provider and CSP2 is an infrastructure provider, then there could be a relationship between CSP1 and CSP2 that might not be known by CSU1 when they acquire the use of CSP1's services. This type of "nested" or layered cloud provider relationship is shown in Figure 3, which makes explicit the possibility of three layers of cloud computing where a SaaS is using a PaaS provider that is contracting out for an IaaS provider to supply the computer and network infrastructure. In Figure 3, the external auditor that is responsible for auditing the CSU is now faced with a need (dotted line) to be aware of, and give opinions on, the external layers of cloud computing services. The auditor's role is complicated by the possibility of limited knowledge of ungoverned cloud relationships, and cases where even governed cloud contracts may limit audit access.

The rest of this section is organized by parties that participate in the cloud ecosystem. Different perspectives for research on cloud computing are discussed from the point of view of the:[4]

1. Cloud service user (CSU) organization (i.e., client)

[4] CSN (as a contracted provider to the CSP to do application development or consulting services) was identified in the cloud ecosystem for completeness, but the CSN is not covered in the subsequent discussion.

2. External auditors (referred to as auditors within this paper)[5]
3. Cloud service provider (CSP) within a governed relationship
4. Investors in the CSU organization (stakeholders)
5. Trading partners of the CSU (stakeholders)
6. End customers of the CSU who may have their own risk, security, and privacy concerns about the focal organization's use of cloud computing services (stakeholders)

This paper puts emphasis on the particular challenges of cloud governance. For example, Figure 2 considers the potential for "relationships made without formal governance approval" (where lines are "X'ed" over, indicating lack of governance oversight). This acknowledges the potential for functional areas or the IT organization to contract directly for cloud services without governance oversight, corporate-level risk assessment, or formal approval. This risk is highlighted in a survey of 613 IT and security practitioners (Ponemon Institute 2014) that found:

- 62 percent do not agree or are unsure that cloud services are thoroughly vetted for security before deployment;
- 69 percent believe there is a lack of proactive assessment to discern what information is too sensitive for storage in the cloud; and
- 63 percent believe there is a lack of audits or assessments of cloud-based services.

The above highlights that cloud computing compliance issues may not have been sufficiently addressed in contract stipulations. Audit and assurance requirements need to be considered early in the cloud contracting process. The following sections identify some of the strategic and managerial issues from the perspectives of different roles within the cloud computing ecosystem.

The Cloud Service User (CSU)

From the perspective of the client organization (CSU) that contracts with a cloud computing services provider (CSP), the following issues are often identified:

- A weak or immature vendor risk management process will likely lead to increased risks associated with cloud computing. The ISACA professional audit organization is recommending guidance based on COBIT 5 (ISACA 2012, 2013, 2014).
- Data will be stored offsite at the CSP (outside the physical boundaries and direct control of the CSU), and they may be stored outside of the country in which the client organization operates. Further, the actual data storage locations may be unknown by the organization that produces, uses, and depends on the corporate data.
- Data controls, security mechanisms, backup activities, and even ownership rights may be obscured and grow fuzzy, as the CSP will likely restrict visibility into the cloud in order to protect the rights, security, and privacy of its other CSUs in a multi-tenancy cloud computing services arrangement.
- Theft of critical data moved to an "offshore" cloud or location might prove to be inaccessible, even for government security or litigation purposes (Risen 2013; Schmitt 2010).
- The critical nature of the CSU-provider relationship creates dependencies. This relationship is likely best built in stages to develop an operational knowledge and trust relationship, starting from less complex and less critical capabilities before becoming heavily vested in critical cloud services (Stamas et al. 2014, 180–184).
- The organization can grow ever more dependent on the information technology expertise of the cloud provider. A concurrent negative effect can be the reduction of internal technology expertise, even though internal IT expertise is needed to monitor and control the CSU–CSP relationship. Such IT expertise is also needed by the organization to implement organization-specific security and privacy protections. This reduction in expertise might lead to a loss in understanding of the strategic IT issues facing the organization.

In order to mitigate the risks associated with the above issues, as well as a broader set of risks suggested in the Taxonomy of Technological IT Outsourcing Risks (Ackermann, Miede, Buxmann, and Steinmetz 2011), the CSU must assess which applications provide critical services or competitive advantage when determining what to move into the cloud. How comfortable is the organization in allowing application processing and data storage to reside outside the organizational boundaries, thereby limiting monitoring and hiding the nature of controls? Being responsible for SOX compliance, HIPPA,

[5] External auditors are the primary means by which the assurance process considered in this paper is performed. There are also other management and assurance-related roles dealing with clouds that are not considered here, such as certification bodies, security consultants, project managers, contract attorneys, etc.

etc., is the CSU organization willing to insert separation between itself as the party responsible for the public trust, from the CSP who directly implements mechanisms for ensuring that trust is maintained?

The Cloud Auditor

Issues that concern the CSU's auditor (ISACA 2011) who acts as an assurance intermediary between the CSU and the CSP include:

- Independent auditors (and internal auditors) of the CSU organization are charged with assurance and attestation responsibilities, but may be restricted from directly auditing the publicly held company's cloud provider. The auditor, who must render an opinion that includes auditing financial information "through the IT systems," may be prevented from directly assessing the controls and security of the cloud services (IT infrastructure, IT systems, and technology support procedures) on behalf of the CSU (e.g., a publicly held corporation undergoing an SEC mandated audit).
- The audit planning phase on behalf of a CSU must consider how to best perform a risk assessment and provide assurance over cloud services from which the auditor is restricted from directly auditing. Special consideration could be needed to determine steps of how to achieve acceptable assurance when the cloud provider's control assurance report is not available, is considered limited, or is deficient.
- The most appropriate standards to address cloud computing may not be universally and consistently agreed upon. Cloud-related standards are evolving and sector-specific needs are emerging, such as restrictions on organizations with government contracts. Compliance standards to address cloud-based IT services should pay specific attention to shared governance issues, independent third-party auditor attestation, and performance of independent testing. Recently evolving standards of note are the SSAE 16 SOC 1 report and AT 101 SOC 2 (AICPA 2015) and SOC 3 reports (ASEC/AICPA 2014); ISAE 3402, *International Standards on Assurance Engagements* (IFAC 2010); COBIT 5 (ISACA 2012, 2013, 2014); and the *USA's Federal Risk and Management Accreditation Program* (FedRAMP 2015a, 2015b) certification as required for U.S. government agencies. FedRAMP standards are based on existing security standards and serve as requirements for cloud contracts from government agencies.
- The auditors for the CSU may find themselves adapting the scale and scope of their audit plan to address CSP audit reports (or lack thereof). Conflicts and incompatibilities may arise when audit planning and judgment are at odds with cloud implementation or ownership boundaries. This can be magnified when the plans for the CSP audit are not adequately considered in negotiating cloud contracts and related agreements. Cloud computing increases the frequency of an auditor seeking another auditor's report (of the CSP) and relying on this third party's attestation (even if it might not meet the scope, depth, or level of reliance and testing as desired by the firm's auditor). The auditor, among other things, provides value by signaling quality, verifying claims and controls, providing audit documentation, and provides an independent evaluation of the CSP (Fairchild 2014). However, to do this effectively and efficiently, the auditor needs for all parties to follow an agreed-upon set of standards so that effective shared governance can be accomplished.

The Cloud Provider

CSPs, as independent legal entities, are situated in a paradoxical role—that of providing critical IT services to publicly held organizations undergoing mandatory audits, but also needing to be treated separately as they service a variety of client organizations. From the CSP's perspective:

- Cloud computing achieves efficiencies by economies of scale in providing a virtualized, dynamic allocation of cloud-based computing services. This model lends preference to standardization of services offered to CSUs. Various cloud providers may differ in the contents of their basic cloud service contract. Baseline expectations of clients likely include a clear statement of ownership rights, data backups, performance levels, a business continuity plan addressing disaster recovery plans, level of privacy, security provided, as well as audit requirements.
- The CSP basic service may not offer assurance. The contract may not have a provision for a direct audit of the cloud by the CSU's independent auditor. The CSP's own audit reports may not be automatically available or routinely disclosed to CSUs.
- CSPs could differentiate levels of service by offering higher-level tiers of service including compliance certifications SSAE 16 SOC 1 report and AT 101 SOC 2 (AICPA 2015) and SOC 3 reports (ASEC/AICPA 2014); ISAE 3402, *International Standards on Assurance Engagements* (IFAC 2010); COBIT 5 (ISACA 2012, 2013, 2014). For contracts with government agencies, the CSU may be required to meet evolving *USA's Federal Risk and Management Accreditation Program* (FedRAMP 2015a, 2015b) standards.
- Privacy and security rights of all the different multi-tenant CSUs must be protected by the CSP. This is a consideration for how to handle, and when to share, cloud audit reports.

- Regarding directly auditing the cloud computing service, the contracted rights of each CSU may vary by type of contract, the cloud model (public, private, and hybrid), and the cloud service (SaaS, PaaS, or IaaS, as well as CSP layers within the cloud). An audit leverage point will most likely be either (1) explicitly including audit terms of the contract with the provider, or (2) selecting a cloud service offering that explicitly commits to provide a sufficient, independent auditor report for inclusion in the client firm's own audit report.

The Cloud Service User Stakeholders

Three stakeholder's perspectives that are indirectly affected by the contracting of cloud computing services by an organization include (1) the shareholders of the CSU who bear financial risk to the company's equity value, (2) the trading partners of the CSU who may have confidential data stored with the CSP, and (3) the end customers of the client organization who may run risks depending on the type and degree of their reliance and dependence on the CSU and data provided to the CSU, which are stored in the CSP's cloud.

Investors in Organizations Using Cloud Services

From the CSU investor's perspective, assurance is needed that their equity investment is not at risk, that the reputation and assets of the organization are safe, and that no excessive risk or liability are incurred due to cloud computing service choices.

- Expectations for disclosure of cloud services contracts and cloud compliance reporting might vary by industry and by CSU size. For example, certain regulated industries, e.g., financial, may have a higher level of reporting responsibility than others, e.g., extractive industries.
- Investors may want to understand which new technology is in use and what organizational capabilities it supports (such as differentiating commodity IT applications from competitive advantage applications of strategic importance).

Customers and Trading Partners

From the CSU customer's perspective, unknowns and risks include:

- The customer is trusting and expecting the CSU to provide an appropriate level of governance and risk containment. The customer does not know the details or the extent of the layers of cloud services in use by the CSU. Yet the customer unknowingly may bear the personal risk of hidden CSP layers if layers are not adequately governed, secured, or audited.
- As customers and trading partners do business with the CSU, they are entrusting that organization with their private data. It may become more difficult to track down customer or partner problems through the layers of outside cloud services that may actually transport, store, backup, secure, and protect the end customer's personal data, financial resources, or archives. If customer or trading partner data are exposed due to a cybersecurity breach, then lawsuits and legal obligations may result. The CSU will need to respond to those lawsuits, as the customers and trading partners have the legal relationship with the CSU (not with the CSP providing the cloud services to the CSU).

Summary Thoughts about the Cloud Ecosystem

The nature of the cloud computing ecosystem calls for extensions to corporate governance and added clarity about shared governance between CSU and CSP, along with the need to establish some sort of shared responsibility between the CSU and CSP. Governance standards place the ultimate responsibility with the board of directors of the CSU, i.e., the cloud client's governance body. Many policies and supporting mechanisms must then be addressed. What parts of the organization are variously responsible for effective execution of governance mandates? How do the CSU and their auditors achieve assurance that the CSP does not add excessive risk? What can be done and who is responsible to respond when the worst occurs—such as a security breach where personally identifiable private information is compromised or critical data are lost?

An effective cloud computing risk governance should be integrated into the existing IT Governance framework. Organizations have a three-layered IT governance structure (De Haes and Van Grembergen 2008). The board of directors is responsible for setting the strategic direction, while the executive management is tasked with overall management and, finally, the line management and IT management are responsible for the operational tasks. This means that all three levels must be involved with cloud IT governance and must understand the implications of cloud computing as it relates to the organization. In particular, effective governance and risk management for cloud computing may not be fully established if there is a lack of board and executive management understanding of cloud computing risks or if the CSU has a deficient vendor management process.

Cloud computing can increase exposure to cyber risk by placing both data and applications, indeed sometimes the entire IT infrastructures, outside the proprietary corporate network. While past forms of IT outsourcing were not immune to cyber risk,

the public forms of cloud computing can push cyber risk to new levels. A 2015 survey of corporate board members (Crowe and Scally 2015) finds the second-highest risk issue[6] is cyber risk, as reported by 80 percent of boards. When asked the question "How confident are you that your board is adequately overseeing cyber risk?" board members' responses showed 23 percent were not confident and 63 percent were only somewhat confident (Crowe and Scally 2015).

III. CLOUD COMPUTING RESEARCH QUESTIONS

There are significant issues related to governance, security, and control within the cloud computing area. The CSU must take the initiative to ensure that governance exists, as "The cloud revolution has raised a fresh set of security, privacy, compliance and risk-management questions. Such is the relative immaturity of the cloud industry that, in many cases, good governance is typically the responsibility of corporate buyers, not cloud providers" (The Economist Intelligence Unit 2014, 9). This section presents cloud governance and assurance research questions organized by CSU activities and responsibilities including strategy, contracting, operations, audit, TCCO (total cost of cloud operations), CSF, and stakeholders concerns. Each research question has a tag identifying the topic and subtopic's question number from the IT Governance framework (Wilkin and Chenhall 2010), where topics include Strategic Alignment (SA), Risk Management (RK), Resource Management (RM), Value Delivery (VD), and Performance Management (PM). As such, this paper outlines a number of key cloud research questions below.

Cloud Computing Governance Related to Strategic Alignment and Risk Management

When considering cloud computing services, it is critical that the strategic decision-making process considers corporate risk and audit requirements. As identified by COSO (2012), early in the process, management must make strategic decisions about the various cloud options (i.e., business process, deployment models, and service delivery models) they wish to pursue. Further, this enterprise risk management approach must consider the unique and shared risks between the internal organization and the CSPs. Each set of strategic design decisions for a cloud-computing architecture sets up future risk profiles for data security and privacy (Halpert 2011; Wood, Brown, and Howe 2013).

The shift to cloud computing is more than just a change of an IT service vendor. It is a fundamental strategic change to (1) the nature of an organization's roles and responsibilities, (2) its technology infrastructure, and (3) the control, monitoring, and assurance of its IT services. The move to cloud computing requires the CSU's governance structure to address a dependent, cooperative relationship to the external cloud provider. Key research questions in this area include:

a. How does use of cloud computing change the nature of IT governance? (SA1) How does the use of cloud computing align with or allow change to the organization's vision and strategies? (SA2)

A fundamental tenet of corporate governance is that IT governance should be aligned with corporate governance. Therefore, consideration of using cloud computing should be driven by the strategic goals of the organization, and should be vetted as part of overall governance activities.

b. How does the oversight role of the board change with the use of cloud computing services? What types of expertise are needed on the board or among its close advisors? (VD3)
c. How should the board be informed by the technology advisory committee and auditor about the technological opportunities and risks of cloud computing? (SA3, SA4)
d. How is governance policy and firm risk appetite (Segal 2006) reassessed, reframed, and/or expanded to adequately address the cloud issues? How does cloud computing change the "risk appetite" of the organization? (RK3)
e. How can the use of cloud computing provide strategic advantage? (SA5) Who within the organization should promote the use of cloud computing? (SA4, SA5) Do the CEO and CIO perceive the same advantages and disadvantages for cloud computing? (SA3, SA4, SA5)
f. Does the CSU's board and executives perform adequate risk assessments of cloud computing and how do these assessments match the organization's risk appetite? (RK1) What are the available strategies and mechanisms to mitigate cloud computing risk, are mitigations proven effective, what are the risk mitigation problems? (RK2)
g. How do organizations vet the decision of which applications to migrate into the cloud, and/or carefully consider the major decision to wholly outsource IT services into the cloud? (SA4, SA5)

[6] This is only behind the top issue of operational risk (reported by 90 percent of boards).

h. Are policies in place to guide decision making that appropriately weight the balance between opportunities facilitated by cloud services against cyber risks and loss of direct technology control and risk of eroding technological competitive advantages when placed in the cloud? (SA7, and all RK)

Yigitbasioglu (2014) identified a negative relationship between perceived vendor opportunism and cloud adoption, and also reported that perceived cloud computing security risk was the leading deterrent to intention to adopt cloud computing.

i. What is contained in a reliable and effective shared responsibility matrix between CSU and CSP? (SA4, SA5, RK2, RK3, RK4, RM2, PM1, PM2, PM3)
j. What mechanisms are needed for cloud security, privacy, monitoring, and control? (SA7, RK2)
k. What is the nature of effective cloud vendor selection and management, especially the process for reviewing and monitoring cloud services? (PM1, PM2, PM3)
l. How can the CSU effectively monitor, control, and evaluate the security, efficiency, and overall success of cloud services? (RM1, RM2, RM6)
m. How well do COSO, COBIT 5, SSAE 16, FedRAMP, as well as other standards and frameworks, support the assessment, management, and control of cloud computing at all levels of the organization? (PM3, PM4, RM1, RM6, RK2)
n. Is the overall cloud computing program considered to deliver sufficient value? How can the value of the cloud computing program be determined? (VD1)
o. What internal processes and strategies (assigning internal roles and external contact points) should be put in place *before* contracting and establishing the CSU's outsourced services? (RK4, RK3, SA2, SA3, SA6, SA7)

Contracting for Cloud Computing Services

The CSU establishes external relationships with CSPs through the contracting phase, but the CSU may be faced with little room for negotiation. Research questions regarding contracting include:

a. How does cloud computing impact the contracting and Service Level Agreement (SLA) process as compared to traditional outsourcing contracts? What types of deficiency penalty clauses are utilized and how can effective monitoring be implemented? (RM6)

Even when monitoring and testing methods are available to check levels of service (Zhang, Ye, Shi, Du, and Guizani 2014), without proper contractual terms, the client would have little recourse when deficient services are identified.

b. How should performance evaluations be incorporated into the cloud service contract? How does the organization evaluate the performance of the CSP? What penalties can be enforced for the failure of the CSP to meet specified service level agreements? Are there specific penalties that result in more favorable outcomes (for the CSU)? (PM1, PM3, PM4)
c. How should policies and procedures be developed for the contracting of cloud computing services that allows the organization to have an appropriate level of risk exposure? (RK1, RK2)
d. How should business continuity plans be coordinated and integrated between the CSP and the internal corporate continuity plan? (RK1, RK2)

The CSU's business continuity planning must be extended to include the cloud. This entails a detailed review of cloud provider disaster recovery plans and robust joint mechanisms to coordinate in disaster situations.

e. What contractual requirements are needed to address timeliness and location of backups, the CSP's ability to provide alternate computing capacity configured for the CSU's use in case of outage, or other service disruption? (RK1, RK2)

Governance of Cloud Computing as It Relates to Operations

The move to cloud computing calls for adapting the CSU's operations to the processes, controls, IT applications, and IT infrastructure of the CSP (Wood et al. 2013). Key research questions in this area include:

a. How does the use of cloud computing change the CSU's internal operations? (RK2, RK4, RM1, RM3, RM4, RM5, RM6)
b. What is a safe and effective staged process to evolve safely into cloud computing relationships with CSPs? (RM-all)[7]

[7] The "RM-all" designation means that all subparts of the RM (Resource Management) topic in the Wilkin and Chenhall (2010) framework are addressed by the tagged statement.

Stamas et al. (2014) reported that a series of developmental cloud adoption cycles over time led to greater integration, tighter coupling, and greater trust across partner organizations. Long-term benefits included improved responsiveness to market opportunities, flexibility, and improved speed at offering new application-based services (Stamas et al. 2014).

c. What new operational job roles and capabilities are needed to effectively manage, monitor, and provide independent controls over the cloud services and protect the CSU's operations? (RM3, RM4, RM5)

A new set of roles may be required for cloud management, requiring strong technical skills for designing controls, performance measurement, and monitoring, along with capability for coordination, interpersonal communication, and complex problem solving. Note that these roles can be difficult to fill as IT expertise may be discouraged when major IT services are moved externally. Rather than reducing dependency on IT expertise, the CSU creates new roles for deep technical expertise to remotely manage the layered external cloud-based IT services.

d. How does the CSU's IT hiring/retention and education process match the strategic vision for the organization as the organization moves toward cloud computing? (RM4, RM5)
e. After entering into Cloud Computing arrangements, what is the degree of risk that a CSU will fail to obtain and retain appropriate IT expertise among in-house staff? (RM3, RM4, RM5)
f. From the perspective of a Balanced Score Card (BSC), what metrics should be used to evaluate the CSP, how should these metrics be collected, and how are they interpreted? How can the CSU effectively monitor performance of the CSP? (PM2)
g. Are decision rights and roles clear within and between organizations? How are end-to-end cloud-related processes best designed? (RM2, RM6)
h. What is the risk of a "shadow cloud" occurring without strategic alignment and hidden from CSU governance bodies? (SA6)
i. What methods and technologies are most effective in monitoring and managing cloud computing remotely? What are the other challenges caused by separation between the CSU and CSP? (PM4)
j. What is the impact and value of requirements that the CSP staff go through to achieve the same level of rigor for hiring and training that the CSU would expect of its staff from its own employment practices (e.g., HIPPA, internal controls, and security)? (RM5)

Governance of Cloud Computing as It Relates to Audit

Cloud computing is a critical audit area given that such arrangements are (1) outside the direct monitoring and control of the client organization; (2) may be multi-tenancy, shared computing platforms; and (3) may be multi-sourced, interlinked layers of computing resources (SaaS, PaaS, IaaS, and other services) spanning cooperating IT providers. As Bapna, Barua, Mani, and Mehra (2010) found, multi-sourcing contains critical interdependent linkages that are absent in a single sourcing environment, which depends on both the primary vendor's efforts as well as the other vendors' supporting efforts. Key research questions related to external audit include:

a. How does cloud computing impact the role of the auditor and audit procedures (traditional attestation)? What robust risk assessment and vendor management processes should be in place for management to follow and auditors to verify? (RK1, RK2, RK3)
b. What is the impact of involving an auditor in the early cloud provider investigation, RPI/RFP/RFQ process, and in the contract negotiation phase? (SA3) What are the benefits and costs of involving the external auditor as an early consultant in governance and strategy issues, prior to the strategic assessment and decision on contracting for cloud computing services? (SA3)

In the early stages of cloud computing arrangements, the auditor could add value in reviewing and updating (1) risk policies, (2) audit expectations, along with (3) control and monitoring plans in preparation for adopting cloud services. The timing of auditor involvement is an interesting construct to research, as audit may not be involved early in the cloud computing contracting phase. There could be impacts on the terms of the contract regarding the segregation of assurance and audit reporting.

c. What is an appropriate delineation of responsibilities and boundaries needed for the separate cloud computing audit entities (as the cloud ecosystem includes the CSU, the CSU's auditor, the CSP, and the CSP's auditor report, if available)? (RK2, RK3, RK4, RM6)

d. How does the external auditor approach the structure and planning of an audit involving CSPs? (RK1, RK2, RM1, RM2, RM6)

Audit planning needs to consider the inherent risk associated with cloud computing and the types of assurance reports provided (if any) by CSPs, determine their adequacy, and possibly specify what other assurance is needed by CSUs. The scope of an audit is of concern because external and internal audit could be limited if contracts do not allow direct audit of the CSP. This limits the audit scope to reliance on the CSP's available audit reports.

e. What is the effect and use of the evolving standards (e.g., COBIT 5, SSAE 16 SOC 1, AT 101 SOC 2 and SOC 3, ISAE 3402, FedRAMP) in audit reports and what other forms of assurance are sought by CSUs' auditors? (RM1, RM2, RM6)
f. To what extent do CSUs consider availability of a CSP's external audit report (e.g., COBIT 5, SSAE 16 SOC 1, AT 101 SOC 2 and SOC 3, ISAE 3402, FedRAMP) to be a requirement before considering the cloud provider? (RK2)

There are a number of important trade-offs to be considered between costs and effectiveness of cloud services. Recently, leading cloud service offerings are answering the call for higher levels of assurance and addressing the need for compliance with various standards (e.g., SSAE 16, SOC 2, HIPPA) (iLand 2016). Because of the multi-client, multi-tenancy structure of a virtualized cloud computing offering, the providers of public cloud services may be inherently limited from allowing the auditor of a CSU from coming inside the CSP's organization in order to continue the client's corporate audit.

g. How should a CSU evaluate the potential gaps between their own organization's internal controls and that of the cloud provider's controls and assurance report (if one is available)? What should a CSU negotiate into their cloud services contract to ensure adequate access to full audit and assurance coverage across the boundary between their own organization and their CSP? (RK2, RK3, RK4, RM2, RM6)
h. How does the location of the financial data (potentially co-located in the cloud and off premises) impact the CSU's audit? (RK1, RK2)

The concept of location itself becomes multi-faceted in cloud environments because it is not just the physical location (or the complexity of identifying and tracking the data's physical location), but also the ability to access the data, as well as access rights (ownership versus custody).

i. How can the CSU best implement their own layer of monitoring and control from outside the cloud as an added level of assurance above those available from the cloud provider? What means are most effective to track and secure cloud-based data as they are maintained and manipulated in the cloud (encrypted, stored, backed up, etc.)? (RK2, RM1, RM6)
j. As cloud service offerings mature, what levels of assurance are needed from CSPs to meet the needs of different types of CSUs? How do different levels of assurance from cloud providers affect CSP pricing? (VD-new)
k. What factors are different between auditing a private cloud maintained by the organization itself versus auditing a private cloud maintained by a CSP? How is each of these types of private clouds impacted by the use of a public cloud in conjunction with each private cloud type? (RK2, RM1, RM6)
l. How can the external auditor effectively provide audit and assurance in a multi-tiered cloud computing environment? (VD-new)

Total Cost of Cloud Operations (TCCO)

The concept of "total cost of ownership" (TCO) is commonly used to encompass the full costs of computing operations. For the cloud computing user organization, it is more appropriate to broaden this concept into "total cost of cloud operations" (TCCO). Cloud computing appears to offer a more predictable cost structure based on the metered and incremental scaling of service offered by cloud providers. Changing IT costs from a capital expenditure (CAPEX) to operating expenses (OPEX) offers operational advantages and may seem to reduce total IT costs. However, in addition to the cost of the cloud computing contract itself, new costs arise when the CSU elects not to own the IT resources but does need to adapt its operations and controls to a cloud environment. Rather than viewing cloud computing as strictly an outsourcing arrangement, placing the critical IT resource in the hands of an external CSP requires extending governance, and therefore requires redesigning many management and operational roles and processes. This creates new direct and indirect hidden costs. Additionally, the tax implications of eliminating the IT hardware (or partially eliminating) needs to be considered. A mature governance structure recognizes that the continued responsibility for overall assurance rests with the CSU that needs to extend its capabilities to maintain overall controls, privacy, security, and monitoring of all cloud computing services. From this perspective, although IT

services can be provided externally, the client company must retain overall control responsibilities. Key research questions in this area include:

a. What are the financial and operational impacts of the change to cloud computing? What are potential realized financial advantages and the hidden financial disadvantages? What aspects and characteristics of cloud computing results in value delivery? What are the real costs, hidden costs (tangible and intangible), as well as savings of engaging a CSP? (VD1, VD2)

A review of ERP cloud use found that cloud ERP reduced client costs (Panorama Consulting Solutions 2015). Does this hold true for a wider set of cloud services and particularly those requiring different levels of assurance and different organizational sizes?

b. What are the tax implications of switching to CSPs from internal IT environments? (RM 6)
c. A benefit of cloud services is to avoid over building IT capacity in order to meet future peak demands. But how vulnerable does this leave the CSU to the CSP's responsiveness in allocating (de-allocating) service capacity quickly enough to meet a sudden increase (decrease) in IT demand? (VD2)
d. How should vendor lock-in to a CSP be addressed? What are switching costs and risks among different CSPs? How should these best be considered when selecting a CSP? (RM6)

Critical Success Factors for Cloud Computing Success

How best can a CSU approach the cloud service acquisition and management process given the potential for high dependency on the CSP? Research questions on critical success factors are:

a. What are the Critical Success Factors (CSFs) for successful cloud computing relationships? Would a general set of IT governance factors be sufficient as CSFs, or what are the added factors unique to cloud computing? (RM1, RM6)
b. To what degree should the CSU's external auditor depend on the CSP's third-party external audit report? What is the degree of effective monitoring, continuity planning, testing, and execution that should be established by the CSU? (RK1, RK2, RK4)
c. What IT and non-IT roles should be centrally involved in the cloud computing service management process? (VD1, VD2, VD3)
d. What is the impact of applying a Capability Maturity Model (CMM) approach within a cloud computing arrangement? (VD1, VD2, VD3)
e. What are the key business processes that benefit the most from CMMs to support a successful cloud computing arrangement? (PM3, PM4)

The approach of assessing individual processes, rather than whole strategies, was supported in a study by Tallon (2007).

f. Would the use of a CMM support in the developing and retaining of key IT computing skills (to avoid loss of IT expertise critical to internal governance, monitoring, and management of cloud computing)? (RM5)

Cloud Stakeholder's Concerns

Key stakeholders (investors, trading partners, and end customers) may be concerned about reliability, privacy, and security risks that may be present in the layers of cloud computing. CSUs need to anticipate and manage their stakeholders' concerns about use of cloud computing. Key research questions in this area include:

a. What disclosures to stakeholders are needed regarding use of cloud computing services? What details are appropriate, such as what CSPs, layers of cloud services from different CSPs providers (e.g., SaaS from one provider that utilizes IaaS service from another provider), the types of applications running in the cloud, and degree of dependency upon specific CSPs (similar to the dependency upon specific trading partners)? (RK1, RK2)
b. Regarding privacy and security, what are the policies, measures, safeguards, and liabilities around cloud computing (e.g., for security breaches, what are the protections in place, how does the monitoring and investigation proceed, and who gets the "black eye" by announcing a security breach)? (RK2, RK3, RK4, RM1, RM6)

CSUs experiencing a major data breach must disclose, but it may well be the CSP who had a security defect or did not recognize the breach in a timely manner.

c. What additional restrictive requirements should be place on the CSU (especially those that extend to CSP) by regulatory agencies (SOX, HIPPA, or FedRAMP) or expected in support of different classes of end customer needs? (SA2, SA4, SA5, RK2, RM1)

d. To ensure data privacy and protection of personally identifiable information, how will CSU business partners be affected when customer and partner data are maintained by the CSU's third-party CSP? In highly integrated interorganizational system collaborations, how will technical support processes best be designed and executed between CSU and CSP? (RM6)
e. Do investors attach greater valuation to CSUs than organizations that do not use cloud services? Do CSUs that use CSPs that publicize certifications (e.g., SOC reports) receive higher valuation than CSUs that use CSPs that do not publicize certifications (or do not have certifications)? (VD-new)

IV. CONCLUSION

This paper focuses attention on pressing research questions related to the governance and assurance aspects of cloud computing. The topic of cloud computing research builds directly on prior work in corporate and IT governance, services auditing, IT outsourcing, multi-sourcing, and IT infrastructure. Yet, this movement into cloud computing takes the CSU into new governance territory of possible elevated risk. Cloud computing risk may not yet have the sufficient understanding or attention of corporate governance bodies. Risk assessments and governance policies must consider how best to share governance responsibilities with cloud providers. Research is needed to better understand the implications of the boundary-spanning nature of the new cloud-based IT infrastructure, an infrastructure that likely involves multiple layers (whereby the primary CSP is utilizing other CSPs).

The cloud computing ecosystem is described to highlight the CSU, their relationships, and interdependencies. What conceptually raises the cloud computing environment from a service infrastructure to the level of an "ecosystem" is the increased degree of shared governance, operational interdependence, and intrinsic cooperation needed in this form of emergent IT services (versus past forms of IT outsourcing). When cloud services are considered, the auditor role provides a beneficial lens to view the CSU to CSP relationship. This lens provides value early in the cloud assessment and adoption process by raising questions of contract responsibilities (both shared and appropriately allocated), compliance standards, audit plans, compliance reporting, disclosures, operational changes, customer support, and disaster recovery. The total cost of cloud operations is addressed because as cloud services are outsourced, overall governance responsibilities dictate that the CSU maintains oversight—thus calling for the CSU to implement some monitoring and a layer of control to ensure managed risk and compliance.

This paper has presented research questions relating to multiple perspectives in the cloud ecosystem spanning from governance, to operations, to audit. The overall intent is to encourage and support investigations in this rapidly growing area of cloud computing services. The main objective is to raise awareness and accelerate investigation into critical cloud computing areas of corporate-level governance, risk management, and responsibilities around cloud audit and assurance. It is important to fully understand the multiple players and hidden layers within each specific client organization's emergent cloud ecosystem.

REFERENCES

Ackermann, T., A. Miede, P. Buxmann, and R. Steinmetz. 2011. Taxonomy of technological IT outsourcing risks: Support for risk identification and quantification. In *Proceedings of the European Conference on Information Systems* (*ECIS)*, Helsinki, Finland, June 9–11.

Amazon.com. 2015. *Introduction to Auditing the Use of AWS*. Available at: http://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf via website: http://aws.amazon.com/compliance/aws-whitepapers/ (last accessed March 16, 2016).

American Institute of Certified Public Accountants (AICPA). 2015. *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)-AICPA Guide*. Available at: http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/IndustryspecificGuidance/PRDOVR~PC-0128210/PC-0128210.jsp

ASEC/AICPA. 2014. *Trust Services Principles, and Criteria*. Available at: http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/Standards/PRDOVR~PC-TSPC13/PC-TSPC13.jsp

Bapna, R., A. Barua, D. Mani, and A. Mehra. 2010. Cooperation, coordination, and governance in multisourcing: An agenda for analytical and empirical research. *Information Systems Research* 21 (4): 785–795.

Briscoe, G., and A. Marinos. 2009. Digital ecosystem in the clouds: Towards community cloud computing. *Proceedings of the 3rd IEEE International Conference on Digital Ecosystems and Technologies,* Istanbul, Turkey, June 1–3. doi: 10.1109/DEST.2009.5276725

Buyya, R., C. S. Yeo, S. Venugogal, J. Broberg, and I. Brandic. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems* 25 (6): 599–616.

Cloud Security Alliance. 2015. *Cloud Controls Matrix v3.0.1*. Available at: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2012. *Enterprise Risk Management for Cloud Computing*. Available at: http://www.coso.org

Crowe, K., and D. Scally. 2015. *What Directors Think: 2015: A Corporate Board Member/Spencer Stuart Survey*. Available at: https://www.nyse.com/WDT2015

De Haes, S., and W. Van Grembergen. 2008. An exploratory study into the design of an IT governance minimum baseline through Delphi Research. *Communications of the Association for Information Systems* 22 (24). Available at: http://aisel.aisnet.org/cais/vol22/iss1/24

Fairchild, A. M. 2014. Patterns of trust: Role of certification for SME cloud adoption. In *Continued Rise of the Cloud: Advances and Trends in Cloud Computing,* edited by Z. Mahmood, 145–158. London, U.K.: Springer-Verlag.

FedRAMP. 2015a. *FedRAMP 3PAO Obligations and Performance Guide*. Version 1.0 (July 29). Available at: https://www.fedramp.gov/files/2015/07/3PAO-Obligations-and-Performance-Guide-v1.0.pdf

FedRAMP. 2015b. *FedRAMP Security Assessment Framework*. Version 2.1 (December 4). Available at: https://www.fedramp.gov/files/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf

Fortis, T., and V. Munteanu. 2014. From cloud management to cloud governance. In *Continued Rise of the Cloud,* 265–287. London, U.K.: Springer.

Grabski, S., and P. J. Schmidt. 2014. Proposing a cloud computing capability maturity model. *Proceeding of the Special Interest Group in Accounting Information Systems (SIG ASYS) Pre-ICIS Conference,* Auckland, NZ, December 13.

Grabski, S., S. 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.

Halpert, B. 2011. *Auditing Cloud Computing: A Security and Privacy Guide 21*. New York, NY: John Wiley & Sons.

iLand. 2016. *Meeting IT Compliance Requirements*. Available at: http://www.iland.com/services/compliance/

Information Technology Governance Institute (ITGI). 2003. *Board Briefing on IT Governance*. Second edition. Available at: http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf

International Federation of Accountants (IFAC). 2010. *Assurance Reports on Controls at a Service Organization*. International Standard on Assurance Engagements (ISAE) 3402. Available at: http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf

International Telecommunication Union (ITU-T). 2012. *Focus Group on Cloud Computing Technical Report*. Available at: https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P1-PDF-E.pdf

ISACA. 2011. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*. Available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx (last accessed May 10, 2015).

ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Available at: http://www.isaca.org/COBIT/Pages/default.aspx (last accessed December 10, 2015).

ISACA. 2013. *COBIT 5 for Assurance*. Available at: http://www.isaca.org/COBIT/Pages/Assurance-product-page.aspx?cid=1001099&Appeal=SEM&gclid=CJa-3fz20MACFSdk7AodbWAAXQ (last accessed March 12, 2016).

ISACA. 2014. *Controls and Assurance in the Cloud: Using COBIT® 5*. Available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx

Iyer, B., and J. C. Henderson. 2010. Preparing for the future: Understanding the seven capabilities of cloud computing. *Management Information Systems Quarterly Executive* 9 (2): 117–131.

Liu, F., J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf. 2011. *NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology*. Special Publication 500-292. Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce.

Mahmood, Z. 2014. *Continued Rise of the Cloud*. London, U.K.: Springer.

Mell, P., and T. Grance. 2011. *The NIST Definition of Cloud Computing, National Institute of Standards and Technology, U.S. Department of Commerce*. Special Publication 800-145. Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce.

Mont, J. 2015. Cloud security is a challenge for users and providers. *Compliance Week*. Available at: https://www.complianceweek.com/news/news-article/cloud-security-is-a-challenge-for-users-and-providers

Panorama Consulting Solutions. 2015. *The 2015 ERP Report*. Available at: http://panorama-consulting.com/resource-center/2015-erp-report/

Pearson, S. 2011. Towards accountability in the cloud: View from the cloud. *IEEE Internet Computing, IEEE Computer Society* 15 (4): 64–69.

Ponemon Institute. 2014. *Data Breach: The Cloud Multiplier Effect*. Available at: https://www.netskope.com/reports/ponemon-2014-data-breach-cloud-multiplier-effect/

Risen, J. 2013. Snowden says he took no secret files to Russia. *New York Times* (October 17). Available at: http://www.nytimes.com/2013/10/18/world/snowden-says-he-took-no-secret-files-to-russia.html

Ritteninghouse, J. W., and J. F. Ransome. 2010. *Cloud Computing: Implementation, Management and Security*. Boca Raton, FL: CRC Press.

Schmitt, E. 2010. In disclosing secret documents, WikiLeaks seeks "transparency." *New York Times* (July 25). Available at: http://www.nytimes.com/2010/07/26/world/26wiki.html?_r=0

Scribd. 2015. *FedRAMP Baseline Security Controls v1.0*. Available at: http://www.scribd.com/doc/77401829/FedRAMP-Baseline-Security-Controls-v1-0#

Segal, S. 2006. Defining risk appetite. *Risk Management* (July): 17–19.

Sotomayor, B., R. S. Montero, I. M. Llorente, and I. Foster. 2009. An open source solution for infrastructure management in private and hybrid clouds. *IEEE Internet Computing, Special Issue on Cloud Computing I* 13 (5): 14–22.

Stamas, P. J., M. L. Kaarst-Brown, and S. A. Bernard. 2014. The business transformation payoffs of cloud services at Mohawk. *Management Information Systems Quarterly Executive* 13 (4): 177–192.

Tallon, P. P. 2007. A process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems* 24 (3): 227–268.

The Economist Intelligence Unit. 2014. *Mapping the Cloud Maturity Curve: The Fundamental Five*. Available at: http://resources.idgenterprise.com/original/AST-0141169_EIU_Fundamental_five_Dec2014.pdf

Truong, H., and S. Dustdar. 2011. Cloud computing for small research groups in computational science and engineering: Current status and outlook. *Computing* 91: 75–91.

Vijayan, J. 2014. *Shadow Cloud Services Pose a Growing Risk to Enterprises*. Available at: http://www.computerworld.com/article/2598551/malware-vulnerabilities/shadow-cloud-services-pose-a-growing-risk-to-enterprises.html

Weill, P., and J. Ross. 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA: Harvard Business School Press.

Wilkin, C. L., and R. H. Chenhall. 2010. A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems* 24 (2): 107–146.

Wood, J., W. Brown, and H. Howe. 2013. *IT Auditing and Application Controls for Small and Mid-Sized Enterprises*. 1st edition. New York, NY: John Wiley & Sons Inc.

Yigitbasioglu, O. 2014. Modelling the intention to adopt cloud computing services: A transaction cost theory perspective. *Australasian Journal of Information Systems* 18 (3): 193–210.

Zhang, H., L. Ye, J. Shi, X. Du, and M. Guizani. 2014. Verifying cloud service-level agreement by a third-party auditor. *Security and Communication Networks* 7 (3): 492–502.

APPENDIX A
A Supplement to Business in the Cloud: Research Questions on Governance, Audit, and Assurance

This supplement organizes and cross-references this paper's cloud research questions into the IT Governance framework (Wilkin and Chenhall 2010).

Cloud_Research_Questions_IT_Govern_Framework_2016: http://dx.doi.org/10.2308/isys-51494.s01