Proposing a Cloud Computing Capability Maturity Model

Pamela J. Schmidt
School of Business
Washburn University
1700 SW College Ave.
Topeka, KS 66621, United States
pamela.schmidt@washburn.edu

Severin V. Grabski
Department of Accounting and Information Systems
Eli Broad Graduate School of Management
Michigan State University
East Lansing, MI 48824-1121, United States
grabski@msu.edu

Proposing a Cloud Computing Capability Maturity Model

Abstract

This research presents a Cloud Computing Capability Maturity Model (CC-CMM) broadly based upon the COBIT 5 (ISACA 2013, 2014) framework and previous well-established capability maturity models (Curtis et al. 1995, 2009; Goldenson and Gibson 2003; Herbsleb et al. 1997; Bate et al. 1995). This CC-CMM is proposed in response to the challenges encountered when applying current IT governance models in the cloud computing environment.

In enterprises with less mature IT governance and risk management, migration of critical applications into the cloud may occur without the executive oversight and without adequate consideration of control and assurance issues. In cloud computing, there is a distributed, arm's-length relationship between the cloud provider and acquiring organization, resulting in the possible migration of IT decision rights to outside the firm. Cloud computing presents a new challenge to IT governance that of shared governance where some IT management and control responsibilities are delegated to the cloud service provider.

We utilize the same maturity level processes (initial, repeatable, defined, managed and optimizing) that are common in the Capability Maturity Model (CMM) literature (Curtis et al. 1995, 2009; Goldenson and Gibson 2003; Herbsleb et al. 1997; Bate et al. 1995). The CC-CMM focuses on issues of risk management in the early stages of considering and selection of cloud services. CC-CMM differs from the CMMI for Services (CMMI Product Team, 2010) which addresses the provision of services rather than the acquisition of services. The CC-CMM focuses on the concerns unique to the cloud computing environment, in particular those relating to governance and security. A defining aspect of the CC-CMM is the reference to COBIT 5 control and assurance recommendations and the inclusion of shared governance for the cloud environments employed by an organization

Proposing a Cloud Computing Capability Maturity Model

1.0 Introduction

This research is motivated by the call for increased involvement in holistic risk management by corporate boards of directors and executive management (Beasley et al. 2009). These demands originate from many fronts including the AICPA, who proposed holistic enterprise risk management (ERM) (COSO 2004, Monda and Giorgino 2013) as the guiding force and initial stage of corporate control and assurance activities; and ISACA, whose update to COBIT 5 increases emphasis on executive leadership and focusing on risks of cloud computing (ISACA 2013, 2014).

In the press, repeated news reports highlight the growing vulnerability of cloud computing. A recent survey of 613 IT and IT security practitioners (Poneman Institute 2014) reports that 66 percent of respondents believe that their organization's use of cloud resources reduces their ability to protect confidential or sensitive information. Further, 63 percent of the respondents believe there is a lack of vigilance in auditing or assessing cloud computing services and 64 percent believe cloud service providers are not fully compliant with privacy and data security regulations. In another survey, 573 business unit executives report that 20 percent of respondents purchased cloud services without the knowledge of the IT department, while 60 percent of the companies had established corporate policies to prohibit this type of purchase (Avanade 2011).

These surveys reveal that, along with a growing trend towards cloud computing, there is a growing trend in abdication of corporate oversight and a reduced ability for the enterprise to have any effective control or assurance related to cloud computing. The last survey's findings imply not only a lack of monitoring by the cloud client but that possibly the ability to monitor the cloud provider activities may actually be blocked or prohibited by the nature of the cloud contract or cloud provider's infrastructure. All these findings reveal serious concerns over IT governance and show a reduction in the enterprise's ability to provide control and assurance as required by their legal and fiduciary duties.

As the practice of cloud computing outsourcing rapidly expands, existing forms and structures of enterprise risk management are challenged in new ways. Cloud computing presents a new challenge in that the organization acquiring cloud services has limited control, lacks direct visibility and has restricted access to the very IT services which they rely upon. If this extreme form of IT outsourcing is not thoroughly vetted at both governance and IT management levels, then the issues of governance, risk management and plans for monitoring and control of cloud computing may be compromised. If managers do not effectively pre-plan for these new risks before contracting with a cloud provider, then it is unlikely that the organization will be able to modify the terms at a later date, nor will the organization likely be able to implement monitoring and control mechanisms after the fact.

The objective of this paper is to develop a Cloud Computing Capability Maturity Model (CC-CMM) to aid organizations in their understanding of risk management as they consider using cloud services. The CC-CMM proposed in this study is based on the risk management capability maturity model (CMM) (Yeo and Ren 2009). Selecting a risk management approach as the

CMM is consistent with recommended approaches (Beasley, Branson and Hancock 2009) including AICPA's Enterprise Risk Management (ERM) (COSO 2004), and ISACA's COBIT 5 (ISACA 2013, 2014). The CC-CMM is proposed in response to the challenges encountered when applying current IT governance models in the cloud computing environment, as those governance models do not directly address the extent of shared governance that exists within the cloud computing environment. This paper assumes the SaaS[1] form of cloud computing in all following discussions. This is done to more fully investigate and specify the need for a CC-CMM to address highest risk instances of cloud computing.

In the remainder of the paper we first provide an overview of the cloud computing environment and issues faced by organizations. We next review some of the capability maturity models and identify the limitations of these models for the cloud computing environment. This is followed by a discussion of IT governance and IT risks within the cloud computing environment. We then present the cloud risk framework. We then use the risk framework and prior capability maturity models to inform the cloud computing capability maturity model that we then present. A design science approach is taken to define the proposed CC-CMM. As part of the CC-CMM, a responsibility assignment matrix is adapted from the Project Management Institute (PMI) and proposed to clarify the roles of partners in shared IT governance. The paper ends with a discussion of future research needs and how the CC-CMM can be used in future research.

2.0 Cloud Computing Environment

The National Institute of Standards and Technology recommends that an organization consider how cloud computing should be deployed, the services provided (obtained), the economic opportunities and risks, the technical considerations, the service level agreements and security of the cloud service (Badger et al. 2012). All deployment models (i.e., software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS) result in similar (but unique) concerns. Rahimli's (2013) findings that cost effectiveness, organizational need, cloud service reliability, and cloud security effectiveness were all significantly and positively related to the cloud adoption decision is consistent with these NIST recommendations.

The utilization of cloud computing services represents a major reduction in the level of visibility and control over the IT computing services for many firms, however, this technology promises increased agility and reduced costs (Golden 2010, Takabi et al. 2010). Cloud computing is different than traditional outsourcing of IT and existing approaches to outsourcing and risk assessment must be expanded to address the inherent risks of cloud computing. A major gap in the current decision making around cloud computing is the overlooking of exposure to increased risks. Cloud outages may be rare, such as the Amazon Web Services failures due to electrical storms or networking events (Clayburn 2012; Miller 2011) or Salesforce.com's storage issue (Kanaracus 2012) and data security and privacy breaches may be less frequent than those reported by non-cloud organization (Balding 2011, Schwartz 2011), but they do occur. Recent privacy cloud issues have been reported related to alleged Twitter (Clearcenter 2014) and iCloud

[1] [1] We focus on SaaS as an exemplar in this research as it is likely the most complex cloud-sourcing environment. That is, an organization contracts with a SaaS provider who subsequently may contract with PaaS and IaaS providers as a means of providing the infrastructure needed for the contracted software services.

service hacks (BBC 2014, HuffingtonPost 2014). As of 2011, 51 per cent of companies reported security concerns as a concern and the primary reason for not adopting cloud computing (Avanade 2011), and almost 25 percent of the surveyed companies had a security breach with a cloud service (Avanade 2011).

In a recent KPMG study (Brown and Fersht 2014), IT managers were asked about their concerns in moving to the cloud. Eighty per cent (of the 740 respondents) were either somewhat or very concerned about data portability if their organization moved to the cloud. Over 70% were concerned about cloud security, and also where the data in the cloud actually would reside.

A growing area of cloud computing is in providing financial, HR/payroll and ERP service offerings (see, for example, SAP, Workday, and NetSuite (Williams 2010)). Cloud services that provide financial information services require compliance with control, audit and assurance regulations. The Sarbanes-Oxley Act requires the CEO and CFO of publically traded firms to attest to the veracity of the financial statements, and 90% of firms required other direct reports, including the CIO, to sign roll-up documents (Bernard 2005). For post-SOX executives to blindly delegate IT governance responsibility outside the firm to a cloud provider exposes the executive and the firm to greater risk than if the IT services were performed in-house. This is a risk that executives appear to have not yet fully realized or addressed as related to cloud computing services.

3.0 Background on Maturity Models

Used as a reference base for CC-CMM, the Software Engineering Capability Maturity Model (CMM^2) is a well-established process improvement model (Paulk et al. 1993, SEI 2002, 2003). Since Software Engineering Institute's (SEI) introduction of the CMM for software in 1993, it has provided a foundation for development of a number of capability models. Various CMM models have been developed and enable organizations to evaluate their maturity in a variety of areas including software development (Herbsleb et al. 1997; Dorfman and Thayer 1997), software acquisition (Ferguson 2002), systems engineering (Bate et al. 1995), integration (SEI 2002), people (Curtis et al. 1995, 2009), supply chain (Lockamy and McCormack 2004; Reyes and Giachetti 2010), project management (Ibbs and Kwack 2000; Crawford 2007), business process (DeBruin and Rosemann 2005), knowledge-based decision making (Kaner and Karni 2004), risk management for complex product systems (Yeo and Ren 2009), and information technology service (Niessink et al. 2002).

A cross-disciplinary comparison of Capability Maturity Models is presented in Table 1 to illustrate both the similarities and differences as the CMM structure has been adapted to various contexts. The table contains brief descriptions of prior CMMs for reference. These established CMM's have been previously developed to address the needs of diverse disciplines, highlighting what differentiates each. The general CMM approach is to define a series of increasing capability levels by which to assess an organizations processes, job assignments, organization structures, measures and innovativeness. Additionally, different CMM's also identify attributes of needed

[2] The SEI Capability Maturity Model (Paulk et al. 1993, 2002) and its successor versions including SEI CMM-Integration (SEI 2002) are collectively referred to by the summary term SEI CMM in this document.

practices, abilities, processes and other factors that support advancement into a higher level of capability maturity.

Empirical research supports the value of achieving higher levels of CMM. In the original area of software engineering CMM, achieving the top maturity of level 5 is found to reduce the variation among software development projects. Organizations at CMM level 5 have software development process under control to the extent that software size (measured by lines of source code) remains the single influential factor in determining software development outcomes of effort, cycle time and quality (Agarwal and Chari 2007). In the supply chain area, research shows that several metrics gathered by higher maturity level firms are significant predictors of performance outcomes (Lockamy and McCormack 2004). Reyes and Giachetti (2010) began validating their supply chain CMM by assessing SCM process maturity level in organizations, and proposing improvements that proved satisfactory to SCM management. Further empirical validation of other CMM's is still needed.

A design science approach (Hevner et al. 2004) has been applied in the development of the various capability frameworks (Becker, et al. 2009). The IT-Capability Model Framework (IT-CMF) provides an archetype of the maturity level of an organization as it implements, improves and controls IT capabilities to support organizational value creation (Curley et al. 2012). The IT-CMF provides organizations an approach to evaluate and manage the IT environment for business value based upon four capabilities: managing IT like a business; managing the IT budget; managing the IT capability; and managing IT for business value (Curley et al. 2012). Across these four areas, organizations evaluate their maturity in 35 critical areas. The IT-CMF is a framework, and as such, must be applicable at a high-level across the organization. However, as the IT-CMF is designed as a high-level framework that is applicable across the organization, it might not fully capture nuanced differences that result from changes in technology, business processes, and governance.

Consequently, we present a Cloud Computing-Capability Maturity Model that is based upon the IT-CMF. The proposed CC-CMM is a "focused area maturity model" (c.f. van Steenbergen, Bos, Brinkkemper, van de Weerd, and Bekkers 2010; Van Steenbergen, van den Berg, and Brinkkemper 2007) that allows for the development and representation of the interdependencies among the processes unique to cloud computing. As a focused area model, the CC-CMM allows for the flexibility and variation needed when dealing with the emerging cloud computing issues and environment which would not be present in a static framework. Mature, fixed level maturity models are more common in well-developed areas including systems engineering (Bate et. al 1995; Dorfman 1997), project management (Ibbs and Kwak, 2000), human resources (people) management (Curtis et al. 1995, 2009 and supply chain (Lockamy and McCormack 2004; Reyes and Giachetti 2010). Over time, as the governance and management of cloud computing matures, it is possible that a more highly structured or "fixed level" maturity model may evolve. In cloud computing's current emergent stage, a flexible focal area maturity model is more applicable.

While cloud computing resources can be acquired by departmental or unit managers in an organization through the use of procurement cards without any significant oversight (Avanade 2011), this type of approach to the acquisition of cloud computing resources may be both risky and contrary to an organization's policies. The use of cloud file services may result in an

organization's violation of governmental export regulations (as the data might be stored on servers in a restricted country). These same services might not have the level of security attached to the provided services that the organization deems necessary. This type of activity within the organization would be indicative of a low level of IT maturity (it could be either slow provision of needed corporate resources or lack of understanding of IT controls or lack of understanding of corporate governance or some other issue). Consequently, organizations need an approach that will allow them to evaluate their relative cloud computing maturity and provide them with a listing of factors to consider. Therefore, the primary objective of this research is to conceptualize and propose a Cloud Computing Capability Maturity Model (CC-CMM). In the development of this model we focus on both the unique aspects of cloud computing and the inherent risks of cloud computing. Similar to Becker et al. (2009), this study takes a design science approach and attempt to develop an innovative problem-solving artifact that will contribute to research. Established risk frameworks and other pronouncements (e.g., COBIT, NIST) are referenced to provide guidance in addition to considering the social aspects of risk management.

4.0 IT Governance

Engaging in cloud computing requires expanding IT governance as well as making fundamental changes to IT risk assessment, controls and auditing. IT governance is defined as "specifying the decision rights and accountability to encourage desirable behavior in the use of IT" (Weill and Ross, 2004, p. 8). Wilkin and Chenhall (2010) state that IT governance also needs to focus on the strategic alignment, risk management, resource management, value delivery and performance measurement of the IT resources. IT governance includes establishing processes and clearly assigning authorities for providing input on IT and making IT decisions. The strategic corporate governance decisions have direct impact on the need for the appropriate strategic alignment of the use of cloud computing resources. Similarly, the risk associated with the use of cloud computing resources that are not under the direct control of the organization must be identified and evaluated. Finally, any outsourced arrangement must include service level agreements and the relevant monitoring arrangements. Clearly, outsourcing IT has implications and, in the case of outsourcing whole IT operations through cloud computing, these implications can be hidden, risky and have broad impacts.

Prior research does not consider new forms of governance which rely heavily on external IT sources to the point of wholly outsourcing IT software, hardware and infrastructure as in SaaS Cloud Computing and which results in delegation of technology design and management decisions to a cloud computing provider. Bardhan et al. (2010) do not consider corporate and IT governance from this perspective. There is no mention of controls or auditing of outsourced cloud services, or of the requirements for the service provider to meet compliance requirements. Akermann et al. (ECIS 2011) present a taxonomy covering technological risk items related to IT security and the quality of service and claim to establish a direct link between technological risks with operational IT security and quality of service aspects. Unfortunately, the business risks associated with cloud computing are not specifically addressed.

Given the fundamental shift in the nature and implementation of IT due to cloud computing, there needs to be an expansion in the understanding of how to handle IT governance in such a setting. Use of cloud computing calls for expanding the basic IT decision archetypes (Weill and

Ross 2004). It is critical to both acknowledge the growth of 'shared IT governance models' and to deliberately design archetype(s) that clarify rights and responsibilities. Lest anyone doubt that cloud computing represents a major shift in IT governance, of the six IT governance decision archetypes identified by Weill and Ross (2004), none delegate any IT governance decisions to entities outside of the firm. The current IT governance model is clearly challenged in handling cloud computing due to the distributed, arm's-length nature of the cloud provider relationship, in which it is possible for IT decision rights to migrate outside the firm.

Organizations rely on IT for critical or strategic applications, and they have a need for a strong IT governance model. Since the cloud computing is relatively new, there is the risk of lax IT oversight, controls and auditing of cloud operations. Consequently, A CC-CMM is vital such that risk and assurance issues be addressed up front. Of particular concern is that audit and assurance may become afterthoughts in the race to implement cost cutting, outsourced relationships. Oftentimes, the final decision as the whether cloud computing resources (SaaS in particular), should be acquired is often driven by economic pressures and operational benefits; governance risks are generally inadequately addressed. Consistent with Wilkin and Chenhall (2010) cloud governance risks should be evaluated based upon strategic alignment with corporate objectives, risk exposures created by the use of cloud services, the management of all corporate IT (and other) assets including data, the value derived from the use of the cloud service provider, and finally, the manner in which the cloud service provider performance will be evaluate (and the associated service level agreements). Specific factors that should be considered include the level of management control and audit visibility into cloud, the service provider's internal controls, and the independent audit of the service provider (such as SSAE 16 (Statements on Standards for Attestation Engagements) and ISAE 3402 (International Standards for Assurance Engagements). Since strategic or critical applications may be placed in the cloud, risk assessments, controls and assurance, and operational service level agreements and plans for external auditing need to be an integral part of the initial cloud computing planning and contracting process.

5.0 IT Risks and Cloud Computing

When using cloud computing services, it is important to understand the layers of services and the service providers employed. SaaS providers often use the services of an IaaS and telecommunications services. This further obscures observability while distributing responsibilities among even more organizations. Who is responsible for ensuring sufficient network capacity, diverse routing and alternatives in case of disaster? In multisourcing arrangements, Bapna et al. (2010) points out that observability and verifiability of outputs has a direct bearing on exposure to risks and the appropriate choice of performance measures. Further, integrated service level agreements (SLA's) which include joint assessments (by client and provider) should lead to better outcomes as agents can observe each other's outputs (Che and Yoo 2001, Ma 1988, Marx and Squintani 2002 as related in Bapna et al. 2010). This approach to proactively managing cloud computing is for the contracting organizations to expand risk assessment, management control and auditing programs and to have an active, up-front role in all cloud decisions and contract negotiations.

Internal control is central to IT governance. Risk assessment and risk containment are central to the control process. Risk assessments identify the likelihood of a threat, the positive and negative

impacts, and possible effects on the organization. *Inherent risk* is defined as the initial risk of the situation before any steps are taken to control either the likelihood or impact of the risk. *Residual risk* is the threat remaining after management has put controls in place or taken other action to address the risk. Corporate governance operates in a cycle that a) assesses the initial, inherent risk of a decision or situation, b) establishes controls and takes other actions to reduce risk to a residual level, c) determines if the residual risk is tolerable and d) if not tolerable, then iterates on the process until risk levels are deemed acceptable. CC-CMM reflects the combination of current joint capabilities of corporate governance and IT governance, the organizations risk appetite and its willingness to absorb risk. This involves, having in place the abilities and processes to mitigate identified risks.

6.0 The Cloud Computing Capability Maturity Model

The proposed CC-CMM (Figure 1) is grounded in the CMM literature. The model contains three dimensions (similar to Reyes and Giachette 2010). These are the CMM levels, the cloud computing capability areas, and the cloud computing types. The maturity levels are consistent with Yeo and Ren's (2009) development of a Risk Management Capability Maturity Model for Complex Product Systems, as integrating cloud computing with on premises computing is a complex task. The cloud computing capability areas are broadly based on COBIT®5 (ISACA 2013, 2014) and Badger et al. (2012). Finally, we apply the maturity levels and competencies across the basic cloud computing types (SaaS, PaaS and IaaS). This paper mainly discusses the SaaS public cloud as the more complex and fully out-sourced form of cloud computing. It is possible for a SaaS public cloud provider to further outsource to a PaaS or IaaS cloud provider, adding nested layers to shared IT governance. Figure 1 is further meant to capture the key dimensions of the CC-CMM, namely the X axis reflects the type of cloud computing (SaaS, PaaS or IaaS); the Y axis represents levels of maturity lifecycle, and the Z axis decomposes the six critical factors based on COBIT 5.

- - Insert Figure 1 CC-CMM Here - -

6.1 Maturity Levels

The CC-CMM proposes five maturity levels (shown in Figure 1 and detailed in Table 2), building upon Yeo and Ren (2009) who based their maturity levels on the ubiquitous software engineering capability maturity model (Paulk et al. 1993). Organizations rated at the two lowest levels (ad hoc and initial) either have not addressed the risks associated with cloud computing or do so only in a rudimentary fashion. There is no overall governance process applied on a consistent manner across the organization. As in other CMMs, level 3 is the "demarcation level." It is at this level that the organization has formalized the assessment of cloud computing risk management, and that the processes are understood throughout the organization. The remaining higher levels (managed and optimizing) result in the organization including and acknowledging key external stakeholders (i.e., both direct and indirect cloud providers – such as the provider of a SaaS and also the IaaS provider used by the SaaS), and also developing continuous process improvements.

6.2 Cloud Computing Capability Areas

There are six cloud computing capability areas (Table 3) based upon COBIT 5 (ISACA 2014) and Badger et al. (2012). These areas include: IT Governance, Management, Data Governance, Security and Reliability, Software and Applications, and Technical. These represent the areas that organizations which acquire cloud services (whether they be for infrastructure, platform or software) need to address potential risks and resources needed. We included the requirement to examine the needed resources, as the lack of resources would expose the organization to unnecessary risks.

6.2.1 IT Governance

IT governance includes both an organization's internal IT governance policies and procedures (COSO 2004, Weill and Ross 2004, Wilkin and Chenhall 2010), and increasingly must also address delegated or shared governance responsibilities with outside entities such as a cloud service provider (ISACA 2011, 2014). This shared governance is needed because it is possible and even likely that IT decision rights migrate outside of the organization to the cloud service provider. For example, the cloud provider determines the hardware and software used and when it will be updated. In SaaS, due to multi-tenancy, multiple organizations are using the same application at the same time. Also, the organization must obtain from the cloud provider any needed assertions regarding the availability, controls and auditability of the system when this is required for governmental reports.

The organization must also determine its risk appetite and overall enterprise risk management (ERM) approach (Rittenberg and Martens 2012). ERM looks at risk from an overall organizational perspective and attempts to align daily operations with the strategic objectives set by the Board of Directors rather than have the organization manage all risks independently from one another (or managed as the risks are identified) (Monda and Giorgino 2013). An organization's optimal level of risk should maximize shareholder value while satisfying the constraints of other stakeholders, e.g., regulatory agencies, customers (Segal 2006). This is then translated by the Board of Directors into the organization's risk appetite, which is a function of the risk exposure and how the organization can respond to risks, whether to mitigate them or to exploit them (Segal 2006). The organization, based upon its risk appetite, manages risk exposure through both strategic (e.g., product mix) and tactical (e.g., computing environment) activities. Risk mitigation occurs when an organization determines how to best offset risk exposures. For example, the loss of product and productivity due to storm or fire damage is often mitigated through the acquisition of insurance.

6.2.2 Management

The management capabilities are based upon the general recommendations for cloud computing (Badger et al. 2012). These include the specification of how data will be both migrated to (and when necessary) from the cloud. The organization must understand what is needed to place the data into the cloud, especially if it is going to be used with a new cloud software as a service rather than a historic on-premises service. Additionally, plans must exist for the retrieval of the data (if a new service would be used or the provider goes out of business). Similarly, the cloud provider's plans for continuity of operations and redundancy plans need to be reviewed. Service

level agreements (SLAs) that specify remediation in case of some type of failure need to be developed as an aspect of continuity of operations, as well as data backup and recovery.

Another capability that must be addressed is the service provider's compliance with controls (e.g., SOX). This may occur through third party audits or may need to be ascertained through some other means. Related to this is the need to gain assurance that the cloud service provider has the appropriate internal controls over their administrative staff to prevent any type of security lapse/breach. These internal controls and need for third party audits (and/or certifications) also exist for the cloud provider's operating policies. The cloud service provider must also possess the capability to provide any needed data based upon ad hoc and formal legal requests, such as discovery proceedings, and must also be able to "freeze" the data (and meta data). Finally, the acceptable use policies must be reviewed and vetted, along with the inclusion of any needed modifications.

6.2.3 Data Governance

The data governance capabilities focus on the security, integrity and access to data placed in the cloud. Regulatory issues and government contracts may restrict movement and storage of regulated forms of data as some data are regulated, cannot leave a particular state/country or cannot be managed by non-nationals where an organization is domiciled. The nature of cloud computing may obscure cloud client's control and monitoring of the handling and storage of critical data. Therefore, the CC-CMM should address the added risk of cloud outsourcing and promote implementation of controls to avoid inadvertent failure to comply with applicable restrictions. These data issues should be considered a priori to contracting, as this issue will rightfully eliminate some cloud providers from being able to offer services to firms with regulatory restrictions. Other issues may also relate to how and where data in the cloud are stored. Organizations must also ascertain that when data it deleted in the cloud, it really is deleted, and that the provider can provide evidence that this has occurred. Organizations must determine who is responsible for backing up (and restoring) the data. Data archiving must also be addressed in great detail to walk the line between data protection and the ability to fully manage data owned by the client firm.

6.2.4 Security and Reliability

The focus of this capability is to ensure that only the organization's specified users can access the data and that the cloud service provider is able to provide the agreed upon services based upon the originally specified performance parameters. Factors related to security include encryption, physical security, authentication, and identity and access management techniques. Performance capabilities include the specification of performance benchmarks (or other key performance indicators) and gaining visibility into the cloud provider's operations as it relates to the organization's data.

6.2.5 Software and Applications

The software and applications capabilities address the differences between the application types that an organization might place into the cloud, and the required performance levels and required support. Time-critical software (e.g., production systems that require precise timing) might not

be appropriate due to the latency associated with cloud applications, whereas these might be appropriate in some private cloud settings. Similarly, safety critical software applications are not recommended for the cloud as organizations cannot validate the entire application provided by a cloud vendor and due to the network variability (Badger et al. 2012).

The cloud service provider needs to assure that all runtime application have been tested and validated. If an organization is using a platform as a service, the code routines called need to perform as intended, and the organization acquiring this service should verify that this works as intended. Finally, cloud service applications should be configurable to run in a secure fashion and they should be able to be integrated with other on-premise (or cloud) services.

6.2.6 Technical

The technical capabilities focus on the use of virtual machines (VMs). An organization must ensure that the cloud service provider can both protect against and detect attacks from other VMs or from wherever the attack occurs. Organizations should also be able to move from one set of VMs with one cloud provider to another (or back on-premises).

6.3 Cloud Computing Types

This research focuses on the three basic cloud computing types: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (NIST 2011). SaaS is the provisioning of software applications on demand, such as e-mail, file storage, financial and customer/supplier relationship applications. PaaS is used for the development of new software applications without the need to acquire and install the hardware and operating system. IaaS is used by organizations to obtain hardware resources that are needed without the need to actually purchase those resources, and with the benefit of cancelling the use of those resources when they are no longer needed, that is IaaS provides the elasticity for needed resources. An additional factor is the choice of public, hybrid or private models of cloud computing. While the proposed maturity model relates to all there types, it is perhaps most valuable in public and hybrid models where there are concerns related to multi-tenancy.

6.4 Responsibility Matrix for Cloud Computing Services

Given the shared governance inherent in using SaaS Cloud Computing, it is essential to establish a comprehensive, up-front assignment of all parties' responsibilities. In order to use the CC-CMM, it is necessary to have a clear understanding of which party is being assessed on each factor in the CC-CMM. The responsibility matrix is the basis for the government, management and monitoring of risks. The responsibility matrix is also required to acknowledge and arrange for the shared nature of internal controls, in order to ensure that the needed audit/assurance will be present when 'doing business in the cloud,' and which party will be responsible for providing that assurance.

Contracts need to specify responsibility and rights for IT controls and auditing the out-sourced cloud activities. This is especially vital when strategic, mission critical or financial business activities are considered for being made cloud-based. In such considerations, internal controls

and auditing functions should be part of the upfront cloud computing decision-making and contract negotiations, with project management centrally engaged in decisions of this nature.

Project management is naturally a focal point of any out-sourcing activity, delegated the role of ensuring the integrity and effectiveness of the outsourced service activity. Therefore, the CC-CMM proposes including a responsibility assignment matrix as adapted from leading project management practices. More specifically, the leading project management professional certification organization, the Project Management Institute (PMI, 2001, www.pmi.org), recommends use of a Responsibility Matrix based on the standard Project Management RACI approach per PMI's Book of Knowledge (PMI-BOK). A responsibility assignment matrix such as a CC-adapted RACI matrix will more clearly identify specify responsibilities as part of the cloud computing relationship to be outlined in the cloud computing services contract and SLA.

There are many reasons why a responsibility assignment matrix is a critical part of the CC-CMM. Shared governance distributes responsibilities unlike traditional in-sourced IT governance where risks are more identifiable, directly observed and internal controls are in control of a single entity. Traditional responsibilities within a single firm are straight forward because the firm's governance group:

1. Have a clear understanding and direct visibility into the practices, controls and assurances within the company.
2. Employee stakeholders directly benefit from the health of the company's operations (vs. out-sourcing companies which do not want to risk a contract's income).
3. A common internal management hierarchical structure exists.
4. The existing risk assessment, management controls, and audit structure are all within the company
5. The company can quickly resolve roles and responsibilities as new issues arise based on existing management responsibilities.

In contrast to a single firm governance environment, there are many significant changes that occur within a shared governance cloud environment. When embarking on an outsourced cloud computing-based (SaaS) environment, there are many reasons to fully specify all the responsibilities and roles of both parties (cloud client and cloud provider) including:

1. Less visibility into the practices, controls and assurances of cloud provider.
2. Cloud provider derives benefits by maintaining contract income even though the service may not be optimal in addressing and protecting all aspects of the client/consumer firm operations.
3. Contract and SLAs govern much of responsibilities and major work tasks in an outsourcing arrangement; therefore need to 'fully' identify responsibilities, activities and effectiveness criteria early during negotiation of the business relationship.
4. Cloud provider has existing set of processes, services and staffing roles assigned which support many customers, therefore they are not as adaptable to individual customer needs or on-going motivation/renegotiation of responsibilities. Utilizing cloud services result in the following:
    a. 'Software version update' decisions are done by the cloud provider with little (no) control/discretion left to cloud consumers.

b. Heightens criticality of up-front decisions and contractual requirements including internal controls, monitoring, reporting and auditing. Such requirements should be based on a full and well-informed risk assessment of the new cloud-based outsourced relationship.
c. Places auditable financial information and IT systems outside the scope of the normal external auditor focus on audited company's internal operations.

Within a SaaS environment, the cloud provider of the software will often use other cloud services, such as IaaS to provide the hardware platform upon which the SaaS resides. This results in a multisourcing arrangement. In multisourcing arrangements, Bapna et al. (2010) points out that observability and verifiability of outputs has a direct bearing on exposure to risks and the appropriate choice of performance measures. Further, integrated SLA's which include joint assessments (by client and provider) should lead to better outcomes as agents can observe each other's outputs (Che and Yoo 2001, Ma 1988, and Marx and Squintani 2002 as related in Bapna et al. 2010.) Bapna's Observablity-Verifiablity Matrix (Bapna et al. 2010, p. 792, Figure 3) is useful in determining an appropriate level of shared governance in a cloud computing outsourcing arrangement.

Verifiable output can be objectively measured regarding its availability and performance response time. Verifiability is an important condition with respect to performance measurements in SLA's. The observability of outputs in aggregate (totals only) versus observability of individual outputs relates to the contracting organization's ability to independently recreate and fully monitor the processing activities of the (cloud) provider. Based on risk levels deemed acceptable to the client firm, the responsibility matrix can be used to determine the various role responsibilities to ensure adequate levels of governance and management are needed to provide adequate assurance to client firm.

In cases with only partially verifiable outputs and /or only totally aggregated output observability, then client governance oversight must be increased – whether by adjustments in cloud provider's processes or by additional governance design by client or jointly. Increasing available options for governance of the cloud provider will likely require additional efforts from both partner's – a need which requires negotiation with the provider who may be reticent to change existing processes already in use with other cloud clients.

7.0 Conclusions

We have presented a proposed cloud computing capability maturity model that is grounded in both the capability maturity model literature and also COBIT 5. A significant contribution of this model is the acknowledgement of a shared governance model that needs to be used in cloud computing environments. As organizations place data into the cloud, they lose physical control over that data and must rely on the cloud provider to properly care for that data. In cloud computing, there is an arm's-length relationship between the cloud provider and organization using that cloud service, resulting in the possible migration of IT decision rights to outside the organization. This results in the need for a shared governance process of how that data will be maintained, processed and protected. Cloud computing presents a new challenge to IT governance that of shared governance where some IT management and control responsibilities are delegated to the cloud service provider.

We utilized the same maturity level processes (initial, repeatable, defined, managed and optimizing) that are common in the Capability Maturity Model literature. Our CC-CMM focused on issues of risk management in the early stages of considering whether and when cloud computing should be used, and also in the selection of cloud services. CC-CMM differs from the CMMI for Services which addresses the provision of services rather than the acquisition of services.

The CC-CMM focuses on the concerns unique to the cloud computing environment, in particular those relating to governance and security. A defining aspect of the CC-CMM is the reference to COBIT 5 control and assurance recommendations and the inclusion of shared governance for the cloud environments employed by an organization. Future research is needed to empirically validate and extend this model, and to also enhance the responsibility matrix for cloud computing.

Table 1
Cross-Disciplinary Comparisons of Capability Maturity Models

Maturity Model Level Definitions	Key defining Characteristics	Level 5	Level 4	Level 3	Level 2	Level 1
SCI's Software Engineering CMM (Herbsleb et al. CACM 1997)	**Initial maturity model, provides foundation for derivative maturity models.**	**Optimizing:** Continuous process improvement is facilitated by quantitative feedback from the process and from piloting innovative ideas and technologies.	**Managed:** measures of software process and product quality, processes and products are quantitatively understood and controlled	**Defined:** Software processes for management & engineering are documented, standardized & integrated. Projects use approved, standard processes.	**Repeatable**: Basic project management processes setup, track cost, schedule & functionality. Process discipline can repeat earlier success on similar applications.	**Initial:** Software process is as hoc, sometimes chaotic. Few processes are defined, success from individual effort and heroics
Project Management Process Maturity PMPM (Kwak and Ibbs 2002)	**Applies original CMM to project management processes**	**Continuous Learning:** innovative Ideas to improve PM Processes and Practices	**Managed at Corp. Level:** Planning and controlling multiple projects in a professional manner	**Managed at Project Level:** Systematic and structured project planning and control for individual project	**Planned:** individual project planning	**Ad Hoc:** understand and establish basic PM principles
IT Service Capability Maturity Model (Niessink, Clerc and van Vliet 2002)	**Based on original CMM, applied to IT service, but lax at lower levels. Emphasis on quantitative measures and their use for process control**	**Optimizing**: Continuous process improvement is enabled by quantitative feedback from the processes and from piloting innovative ideas and technologies.	**Managed**: Measurements of IT service delivery process & quality are collected. Both service processes & delivered services are quantitatively understood and controlled.	**Defined**: IT service processes are documented, standardized, and integrated into standard service processes. Services use approved, tailored versions of standard processes.	**Repeatable**: Basic service management processes are established. The necessary discipline is in place to repeat earlier successes on similar services with similar service levels	**Initial**: The IT service delivery process is ad hoc, & may be chaotic. Few processes are defined, and success depends on individual effort and heroics.

Supply Chain Process Maturity Model (SCPMM) (Lockamy and McCormack 2004)	**Applies and extends original CMM beyond the enterprise, including external partners in collaborative joint processes. Implies CMM value begins at level 3.**	**Extended:** Competition based on multi-firm networks. Collaboration between legal entities is routine. Trust and mutual dependency, Horizontal, customer focused	**Integrated**: Cooperation at the process level. Org structures and jobs are process oriented. Process measures deeply embedded. Advanced process management practices.	**Linked:** "Breakthrough level" Managers strategically deploy process management. Broad process jobs & structures exist outside functions. Cooperating vendors & customers, measurement.	**Defined:** Basic processes are defined and documented, changes go through formal procedure. Jobs and org. structures include a process aspect but basically traditional. Functional area reps meet to coordinate.	**Ad Hoc:** Process are unstructured, ill-defined, & without measures. Jobs and org. structures based on traditional functions, not horizontal processes. Heroics and workarounds achieve results.
Business Process Management maturity model (DeBruin and Rosemann 2005)	**Retained CMM levels, focus on factors & to explicate more detailed level definitions.**	**Optimizing (Leader)**	**Managed (Performer)**	**Defined (Achiever)**	**Repeatable (Improver)**	**Initial (Learner)**
Risk Management Capability Maturity (RM-CMM) for CoPS (Complex Product Systems) (Yeo and Ren 2009)	**Applies CMM to risk management for complex products, thus extending CMM to top management by applying a CMM to governance at executive & board level. Implies CMM value begins at level 3.**	**Optimizing:** Continuous process improvement to improve RM performance is the norm. Partnerships with external stakeholders and government agencies are in place. Business risks are considered seriously in decision making.	**Managed:** Corporation has a "Risk-awareness mindset". Measureable risk management process goals. Quantitative measures of risk impact and severity. Extended activities to stakeholders and suppliers, contractors, etc. Uses institutional arrangements.	**Defined**: Demarcation Level: Formal Risk Management system within business processes, benefits understood executives. Measure risk probability, impact & severity. Risk owners are identified and project managers handle most known or predictable risks.	**Repeatable**: Only basic risk management activities performed as part of Project Management. Only rudimentary project risk management systems in place. No organization-wide Risk Management	**Initial:** Unaware of need for risk management, no structured approach to risk. Reactive and mechanical mindset without future planning

Supply Chain Management maturity model (Reyes and Giahetti 2010)	**Extends CMM to suppliers & customers. Focus: measures & collaborative processes. Higher expectations for levels 2 & 3.**	**Leading**: Enterprise has established procedures to collaborate with suppliers and customers. Does measure practices, obtains feedback to continually improve	**Collaborative**: Enterprise has established procedures to collaborate with suppliers and customers	**Manageable**: Enterprise has established procedures that they measure and manage to measurements. Integrates & coordinates internal processes & systems	**Defined**: Enterprise has defined the process and procedures. But competency areas are isolated and there is little formal efforts to integrate the many processes	**Undefined**: Enterprise has no documentation or standardization. Processes are ad hoc, dependent on the person doing the activity, and reactive to the environment

Table 2
Cloud Computing – Capability Management Maturity Levels[3]

Level 1: Ad Hoc	Organization is unaware of the need to manage cloud computing risk. Issues are addressed in an ad hoc fashion as they arise. No governance processes exist.
Level 2: Initial	Some risk management processes exist with respect to cloud computing. The organization is aware of potential benefits of cloud-computing risk management but does not have the ability to implement them.
Level 3: Defined	The organization has a formal governance process to address cloud computing risks and this is implemented across the organization. A training program has been implemented across the organization to ensure managers and others have the appropriate knowledge with respect to cloud computing risks and how these should be addressed.
Level 4: Managed	Measureable process goals related to cloud computing and the associated risk management are defined. The processes include the identification, assessment and response to the incurred or potential risks. Risk mitigation processes and strategies are identified.
Level 5: Optimizing	A comprehensive cloud computing risk management plan with associated measures exists. Continuous process improvement to achieve higher levels of performance exist.

[3] Based upon Yeo and Ren (2009)

Table 3
CC-CMM Capability Areas[4]

1. IT Governance
   a. Board of Directors IT governance
   b. Executive (Internal) IT governance
   c. Shared (Delegated) IT governance
   d. Alignment with risk appetite
   e. Capabilities for risk mitigation

2. Management
   a. Data migration (to and from)
   b. Continuity of operations
   c. Compliance with controls (e.g., SOX)
   d. Administrative staff
   e. Legal
   f. Operating policies
   g. Acceptable use policies

3. Data Governance
   a. Data access
   b. Data separation
   c. Data integrity
   d. Data disposition
   e. Data regulations
   f. Data recovery

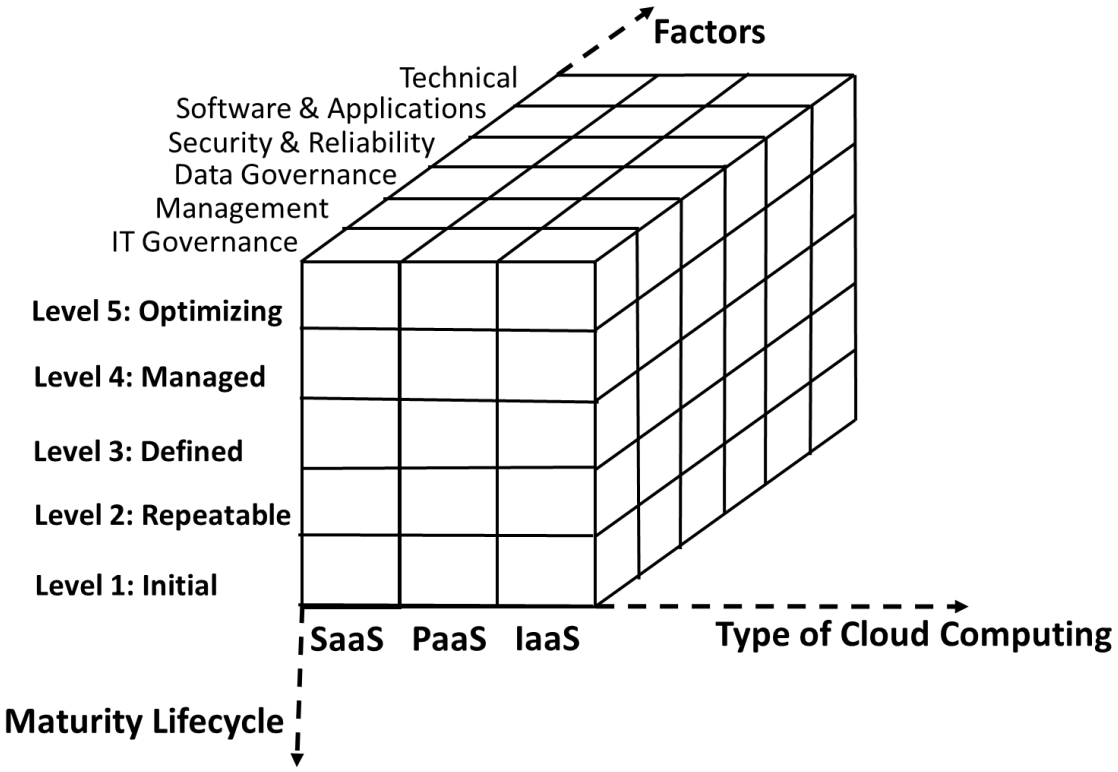
4. Security and Reliability
   a. Encryption
   b. Physical security (on-premises and at cloud provider)
   c. Identity and access management
   d. Authentication
   e. Performance requirements
   f. Visibility

5. Software and Applications
   a. Time-critical software
   b. Safety-critical software
   c. Application runtime support
   d. Application configuration

6. Technical
   a. VM vulnerabilities
   b. VM migration

[4] Based, in part, upon ISACA's Controls and Assurance in the Cloud: Using COBIT 5 (2014) and Badger et al. (2012)

Figure 1
Cloud Computing – Capability Maturity Model Structure



References

Agrawal M, and Chari K. Software effort, quality, and cycle time: A study of CMM level 5 projects. IEEE Transactions on Software Engineering 2007;33(3):145-156.

AICPA. Service Organization Controls: Managing Risks by Obtaining a Service Auditor's Report. 2010.

AICPA. Service Organization Controls: Managing Risks by Obtaining a Service Auditor's Report. Whitepaper 2013.

Avanade. Global Survey: Has Cloud Computing Matured? Whitepaper 2011. http://www.avanade.com/Documents/Research%20and%20Insights/FY11_Cloud_Exec_Summary.pdf

Badger,L, Grance, T, Patt-Corner R, Voas, J. Cloud Computing Synopsis and Recommendations. NIST Special Publication 800-146. 2012.

Balding C. GoGrid Security Breach. http://cloudsecurity.org/blog/2011/03/30/gogridsecurity-breach.html, CloudSecurity.Org 2011.

Bapna R, Barua A, Mani D, Mehra A. Cooperation, Coordination, and Governance in Multisourcing: An Agenda for Analytical and Empirical Research. Information Systems Research 2010;21(4):785–795.

Bardhan I R, Demirkan H, Kannan P K, Kauffman R J, Sougstad R. An Interdisciplinary Perspective on IT Services Management and Service Science. Journal of Management Information Systems 2010;26(4):13–64.

Bate R, Kuhn D, Wells C, Armitage J, Clark G, Cusick K., Hanna M, Jones R., Malpass P, Minnich I, Pierson H, Powell T, Reichner A. A Systems Engineering Capability Maturity Model, Version 1.1. Software Engineering Institute, Carnegie Mellon University 1995.

BBC News. Apple confirms accounts compromised but denies security breach. Posted Sept. 2, 2014, Accessed 9/7/14. http://www.bbc.com/news/technology-29039294

Beasley M S, Branson B C, Hancock B V. ERM: Opportunities for improvement: take your risk management system to the next level. Journal of Accountancy 2009;208(3):28-32.

Becker J, Knackstedt R, Pöppelbuß D W I J. Developing maturity models for IT management. Business & Information Systems Engineering 2009;1(3):213-222.

Bernard A. Sarbanes-Oxley Could Send You to Jail. CIO 2005. Accessed Oct. 5, 2011 at http://www.cioupdate. com/insights/article.php/3513481/Sarbanes-Oxley-CouldSend-You-to-Jail.htm

Brown D, Fersht P. Executive Report: The State of Services & Outsourcing in 2014. *KPMG* 2014. accessed November 5, 2014, http://www.kpmg-institutes.com/content/dam/kpmg/sharedservicesoutsourcinginstitute/pdf/2014/state-of-outsourcing-2014-exec-findings-hfs.pdf

Clayburn T. Amazon Web Services Hit by Power Outage. InformationWeek 2012. http://www.informationweek.com/news/cloud-computing/infrastructure/240002170

COSO. Enterprise Risk Management – Integrated Framework, Executive Summary. Sept. 2004.

COSO. Enterprise Risk Management for Cloud Computing. June 2012.Accessed Sept. 12, 2014. http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf,

Crawford J K. Project Management Maturity Model. New York: Auerbach Publications; 2007.

Curley M, Kenneally J, Dreischmeier R. Creating a New IT Management Framework Using Design Science. In Practical Aspects of Design Science. Berlin Heidelberg: Springer; 2012; 96-115.

Curtis B, Hefley W E, Miller S. Overview of the People Capability Maturity Model. Software Engineering Institute, Carnegie Mellon University, 1995.

Curtis B, Hefley B, Miller S. People Capability Maturity Model (P-CMM) Version 2.0 (No. CMU/SEI-2009-TR-003). Carnegie-Mellon University of Pittsburgh PA, Software Engineering Institute 2009.

DeBruin T, Rosemann M. Towards a Business Process Management Maturity Model. In Bartmann D, Rajola F, Kallinikos J, Avison D, Winter R, Ein-Dor P, et al. (Eds.) ECIS 2005 Proceedings of the Thirteenth European Conference on Information Systems 2005;26-28. Germany, Regensburg. http://eprints.qut.edu.au/25194/

Dorfman M, Thayer R H. The capability maturity model for software. Software Engineering 1997;427-38.

Ferguson J R. Software Acquisition Capability Maturity Model. Encyclopedia of Software Engineering. Wiley & Sons; 2002

Golden B. Cloud Computing: Two Kinds of Agility. CIO.com July 16, 2010. Accessed Oct. 2, 2014. http://www.cio.com/article/599626/Cloud_Computing_Two_Kinds_of_Agility

Goldenson D R, Gibson D L. Demonstrating the Impact and Benefits of CMMI: An Update and Preliminary Results. Software Engineering Institute, Carnegie Mellon University 2003.

Herbsleb J, Zubrow D, Goldenson D, Hayes W, Paulk M. Software Quality and the Capability Maturity Model. Communications of the ACM 1997;40(6):30-40.

Hevner A R, March S T, Park J, Ram S. Design Science in Information Systems Research MIS Quarterly 2004;28(1):75-105.

HuffingtonPost. http://www.huffingtonpost.com/2014/08/31/jennifer-lawrence-nudephotos_n_5745260.html, 2014.

Ibbs C W, Kwak Y H. Assessing project management maturity. Project Management Journal 2000;31(1):32-43.

ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. 2012, http://www.isaca.org/COBIT/Pages/default.aspx

ISACA. COBIT 5 for Assurance.2013. http://www.isaca.org/COBIT/Pages/Assurance-product-page.aspx?cid=1001099&Appeal=SEM&gclid=CJa-3fz20MACFSdk7AodbWAAXQ

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

ISACA. IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. 2011. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx

ISACA. IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. Rolling Meadows, IL. 2011.

Kanaracus C. Salesforce.com Hit with Outage. Computerworld.com June 28, 2012. Accessed Sept. 12, 2014. http://www.computerworld.com/s/article/9228616/Salesforce.com_hit_with_outage?source=CTWNLE_nlt_entsoft_2012-07-02&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+computerworld%2Fs%2Ffeed%2Ftopic%2F120+%28Computerworld+CRM+News%29, 2012

Kaner M, Karni R. A capability maturity model for knowledge-based decision making. Information, Knowledge, Systems Management 2004;4(4):225-252.

Kwak Y H, Ibbs, C W. Project Management Process Maturity (PM) Model. Journal of Management in Engineering 2002;18(3):150-155.

Lockamy, III A, McCormack K. The Development of a Supply Chain Management Process Maturity Model Using the Concepts of Business Process Orientation. Supply Chain Management: An International Journal 2004;9(4):272-278.

Miller R. Major Amazon Outage Ripples Across Web. Data Center Knowledge 2011. http://www.datacenterknowledge.com/archives/2011/04/21/major-amazon-outageripples-across-web/

Monda B, Giorgino M. An ERM Maturity Model, 2013 Enterprise Risk Management Symposium. Chicago, IL. April 22-24, 2013.

Niessink F, Clerc V, van Vliet H. The IT Service Capability Maturity Model. Software Engineering Institute, Carnegie Mellon University, 2002.

NIST. Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53. 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST. Special Publication 800-145: The NIST Definition of Cloud Computing. Sept. 2011.

Paulk M C, Curtis B, Chrissis M.B, Weber C V. Capability Maturity Model for Software, Version 1.1. Software Engineering Institute, Carnegie Mellon University, 1993.

Paulk M C, Weber C V, Garcia S M, Chrissis M B, Bush M. Key Practices of the Capability Maturity Model, Version 1.1. Software Engineering Institute, Carnegie Mellon University, February 1993.

Poneman Institute, Data Breach: The Cloud Multiplier Effect. 2014. http://go.netskope.com/rs/netskope/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf

Project Management Institute (PMI). Project Management Body of Knowledge (PMBOK® GUIDE) 2001.

Rahimli A. Factors Influencing Organization Adoption Decision On Cloud Computing. International Journal of Cloud Computing and Services Science (IJ-CLOSER) 2013;2(2):140-146.

Reyes H G, Giahetti R. Using Experts to Develop a Supply Chain Maturity Model in Mexico. Supply Chain Management: An International Journal 2010;15(6):314-424.

Rittenberg D L, Martens F. Enterprise Risk Management: Understanding and Communicating Risk Appetite. COSO Jan. 2012.

Romney M B, Steinbart P J. Accounting Information Systems. New Jersey: Prentice Hall; 2011:697.

Schwartz M J. 6 Worst Data Breaches of 2011. InformationWeek.com 2011. Accessed Sept. 21, 2014. http://www.informationweek.com/news/security/attacks/232301079

Segal S. Defining Risk Appetite. Risk Management 2006;July:17-19.

SEI. Capability Maturity Model Integration (CMMI SM), Version 1.1. CMMI SM for Systems Engineering and Software Engineering (CMMISE/SW, V1. 1), Staged Representation. CMU/SEI-2002-TR-002, ESCTR-2002-002, 2002.

Takabi, H, Joshi J B D, Ahn G. Security and Privacy Challenges in Cloud Computing Environments. Security and Privacy IEEE 2010;8(6):21-31.

Team C P. CMMI for Services, Version 1.3. 2010.

Team C P. CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1. Continuous Representation. CMU/SEI 2002.

Van Steenbergen M, Bos R., Brinkkemper S, van de Weerd I, Bekkers W. The Design of Focus Area Maturity Models, in Global Perspectives on Design Science Research, 5 International Conference, DESRIST 2010, St. Gallen, Switzerland, R. Winter, J.L. Zhao, and S. Aier (Eds.), Lecture Notes in Computer Science 6105, Springer; 2010:317-332.

Van Steenbergen M, van den Berg M, Brinkkemper S. A Balanced Approach to Developing the Enterprise Architecture Practice. in Enterprise Information Systems, 9th International Conference, ICEIS 2007, Funchal, Portugal, Filipe, J., Cordeiro, J. and Cardoso J. (Eds.), Lecture Notes in Business Information Processing 12, Springer 2007:240-253.

Vijayan J. Twitter Breach Revives Security Issues with Cloud Computing, ComputerWorld 2014; accessed Nov. 9, 2014. http://www.computerworld.com/article/2526154/security0/twitter-breach-revives-security-issues-with-cloud-computing.html

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

Wilkin, C.L. and Chenhall, R.H. A Review of IT Governance: A Taxonomy to Inform Accounting Information Systems, The Journal of Information Systems 2010 24(2): 107-146.

Williams M I. A Quick Start Guide to Cloud Computing. London: KoganPage; 2010.

Yeo K T, Ren Y. Risk Management Capability Maturity Model for Complex Product Systems (CoPS) Projects. Systems Engineering 2009;12(4):275-294.