A Comparison of IT Governance and Control Frameworks in Cloud Computing

Completed Research Paper

Elana Bailey
Information Technology & Decision Sciences Department
University of North Texas
e.bailey@live.com

Jack D. Becker
Information Technology & Decision Sciences Department
University of North Texas
becker@unt.edu

Abstract

Providing the appropriate level and type of IT governance and controls in a cloud computing environment is a new challenge facing many CIOs and their organizations. This paper provides a comparison of several of the existing control frameworks, including: CobiT, COSO, ITIL, ENIA, and ISO 27000. While there are many commonalities among these frameworks, the authors identify the key components of each model as they relate specifically to the cloud computing environment. Governance in the cloud requires defining policies and implementing an organizational structure with well-defined roles for the responsibility of information technology management, business processes, and applications. Best practice IT governance considerations proffered by Weill and Ross, ITGI, and others are then included into our cloud framework. Finally, the IT Cloud Governance Dial is presented in this paper, which identifies the necessary steps for implementing the appropriate IT governance for a cloud environment.

Keywords

IT Governance, Cloud Computing, CobiT, COSO, ITIL, ENISA, ISO 27000/9000, Risk Management

Introduction

Cloud computing is a significant information technology trend that has expanded the scope and role of IT governance. According to the IT Governance Institute (ITGI), 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, 2012). Information technology governance is a subset discipline of corporate governance that focuses on the performance and risk management of IT systems. Due to compliance initiatives such as Sarbanes-Oxley and HIPPA, the interest in IT governance has increased. Information technology governance seeks to assure that IT investments produce business value as well as mitigate the risks that are associated with IT. Governance in the cloud requires defining policies and implementing an organizational structure with well-defined roles for the responsibility of information technology management, business processes, and applications as these elements are moved out of the traditional IT environment and into the cloud.

Current IT Standard/Control Frameworks and Models for Cloud Governance

Understanding the standards and frameworks that apply to IT governance is a prerequisite to any discussion of governance in or with the cloud. Several popular IT Governance and Standards Frameworks are displayed in Figure 1: COSO; CobiT; ITIL, and ISO 27001/9000. While no one framework or model

encompasses all of the possible IT controls, collectively they cover the "what, how, and scope" of IT Governance — albeit with some duplication and overlap.

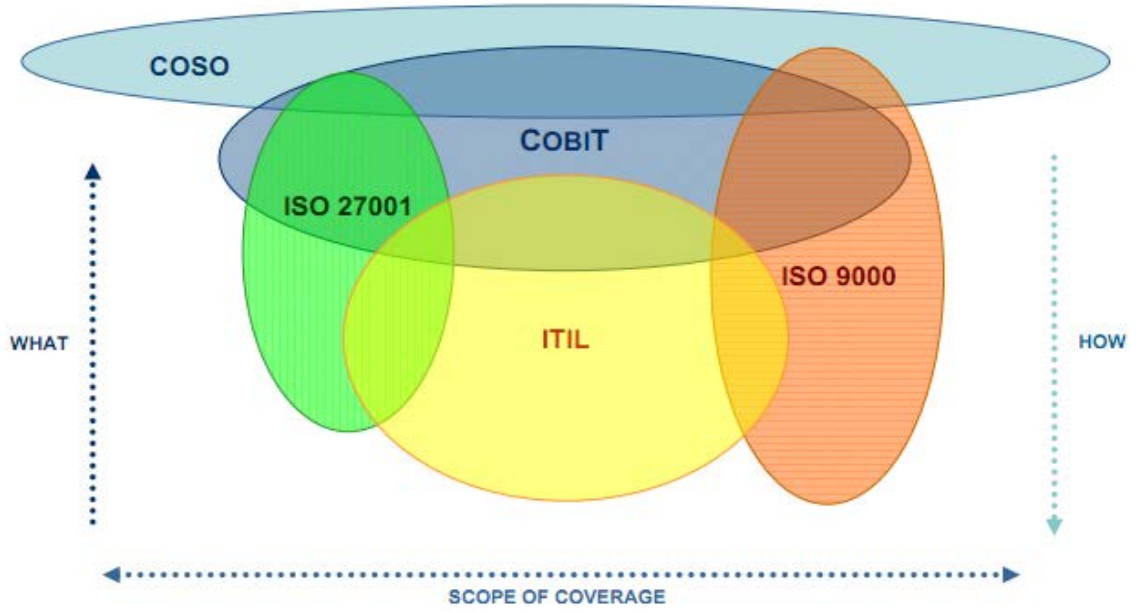

Figure 1: Framework relationships (Nguyen, 2010)

The introduction of cloud services into the IT function does not change the purpose of established standards and frameworks. It does, however, require an extension to include the unique elements of applying IT governance to third party service providers. Although cloud computing creates new opportunities it also creates new risks. In order to reduce these risks, cloud providers and clients must work collaboratively to provide an assurance framework. Many respected IT organizations and standards setting bodies have established frameworks to identify the "risks and mitigation strategies with the evolving cloud computing paradigm" (Crowe Horwath LLP, Chan, Leung, & Pili, 2012). The following sections discuss these five frameworks in further detail as well as the Jericho Forum Cloud Cube Model.

CobiT (ISACA)

In 2011, the Information Systems Audit and Control Association (ISACA) published "IT Control Objectives for Cloud Computing" to facilitate the understanding of cloud computing and the associated risks. ISACA is the organization behind CobiT. Control Objectives for Information and Related Technology (CobiT) is an IT governance control framework that helps organizations address the areas of regulatory compliance, risk management and aligning IT strategy with organizational goals. The model presented in Figure 2 depicts the various elements and dimensions of cloud architecture.

Service Delivery Models

Cloud computing traditionally provides three delivery models: SaaS, PaaS, and IaaS.

- **SaaS** – Software-as-a-Service provides cloud hosted business applications to users using a thin client or web browser.
- **PaaS** – Platform-as-a-Service delivers operating systems, storage and network capacity via the internet.
- **IaaS –** Infrastructure-as-a-Service is the outsourcing of hardware and other operation support equipment such as storage, network components, and servers. IaaS is also referred to as Hardware-as-a-Service (HaaS).

Expanded delivery models now include **BPMaaS**.

- **BPMaaS** – Business-Process-Management-as-a-Service "provides the complete end-to-end business process management needed for the creation and follow-on management of unique business processes" (Fingar, 2010).

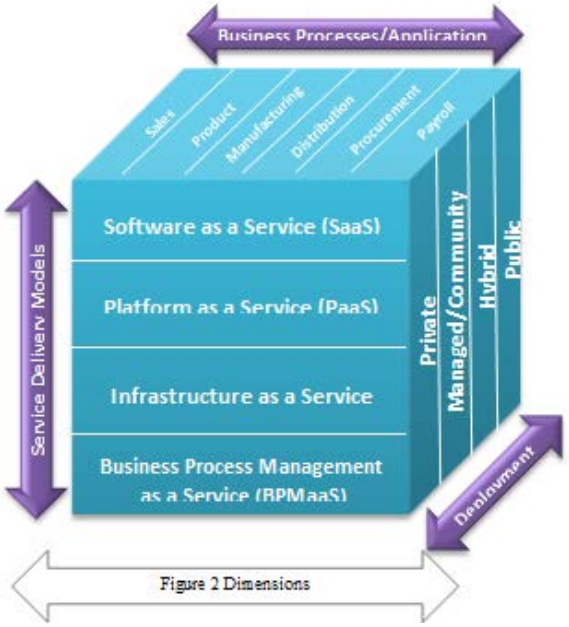

Figure 2: Cloud Computing Service Delivery and Deployment Model
(Adapted from the Cloud Computing Service Delivery and Deployment Model to include the BPMaaS delivery mode, Cloud Security Alliance, *https://cloudsecurityalliance.org, 2009*)

Deployment Models

- **Private –** a single enterprise user
- **Managed/Community** – specific tools and applications supplied to affiliated users
- **Hybrid** – users optimize the advantages of two or more deployment models
- **Public –** communal sharing of applications, processing and data storage

The ISACA audit and assurance program includes an enterprise risk management framework to identify security risks and mitigate vulnerabilities. In 2012, ISACA released CobiT 5 which is "designed to integrate other approaches and standards including TOGAF[1], PMBOK[2], Prince2[3], COSO, ITIL, PCI DSS[4], the Sarbanes-Oxley Act[5] and Basel III[6]" and considers key business and technology issues such as cloud

[1] "The Open Group Architecture Framework (TOGAF®) is a framework for enterprise architecture which provides a comprehensive approach for designing, planning, implementing, and governing an enterprise information architecture. TOGAF is a registered trademark of The Open Group in the United States and other countries" (Wikipedia).

[2]" The Project Management Body of Knowledge (PMBOK) is a collection of processes and knowledge areas generally accepted as best practice within the project management discipline" (Haughey).

[3] "PRINCE2 (an acronym for projects in controlled environments, version 2) is a project management methodology" (Wikipedia).

[4] "The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards" (Wikipedia).

[5] "The Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms" (Wikipedia).

computing (Cole, 2012). Evidence of this integration is illustrated by the similarity of elements appearing in the ISACA CobiT model and COSO and ENISA models discussed below.

Cloud Cube Model (Jericho Forum)

The Jericho Forum [7] **Cloud Cube Model** (JerichoForum.org) identifies criteria with which to differentiate cloud formations from each other and to assist in determining which formation is best suited to the business's needs (Rebollo, Mellado, & Fernandez-Medina, 2012). The model shown in Figure 3 consists of four dimensions:

1. Internal/external – physical location
2. Proprietary/open - ownership
3. Perimeterised/de-perimeterised - collaboration
4. Insourced/outsourced – delivery management

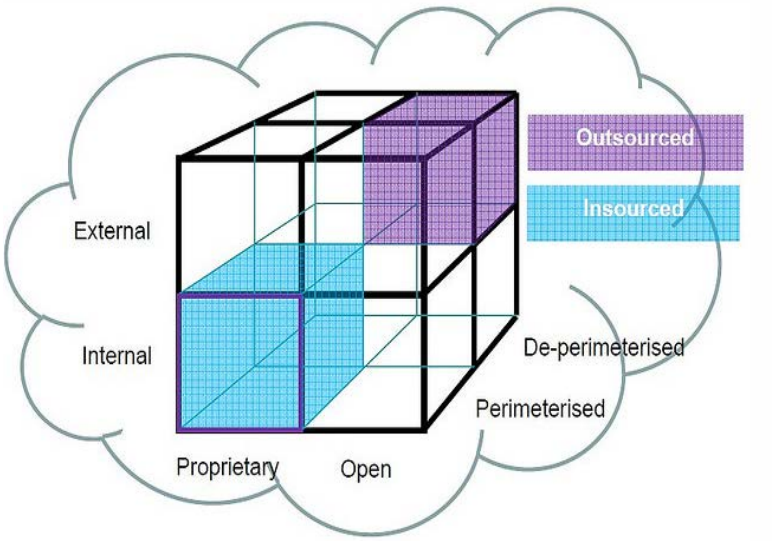

Figure 3: Jericho Forum Cloud Cube Model
Source: www.jerichoforum.org

Internal/external: defines the physical location of the data, i.e. inside or outside the organization's boundaries.
Open/proprietary: defines the ownership of technology, services, and interfaces and depicts the interoperability between the clients systems and other cloud forms.
Perimeterised/de-perimeterised: represents the "architectural mindset". Traditional perimeters are evidenced by the presence of measures securing organizational borders (boundary between corporate network and the internet). De-perimeterised describes the extent to which collaboration or data sharing outside the organizational borders is facilitated.
Insourced/outsourced: identifies who is managing the delivery of the cloud services – third party provider or your own IT staff. This dimension is identified by color (blue = insourced, purple = outsourced) and either color can appear in any quadrant of the model.
Selecting the appropriate cloud formation and understanding the security risks of that selection enable users to develop a set of guidelines to secure interaction between users and end systems located in different security domains (Rebollo, Mellado, & Fernandez-Medina, 2012).

---

[6] "**Basel III** (or the Third Basel Accord) is a global, voluntary regulatory standard on bank capital adequacy, stress testing and market liquidity risk" (Wikipedia).

[7] "The Open Group Jericho Forum® is the leading international independent group of information security thought-leaders dedicated to advancing secure business in global, open-network environments" (opengroup.org) .

COSO – ERM Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) applies their Enterprise Risk Management (ERM) framework to cloud computing as shown in Figure 4. The Cloud Options described in this framework were first introduced in the ISACA CobiT model in Figure 2.

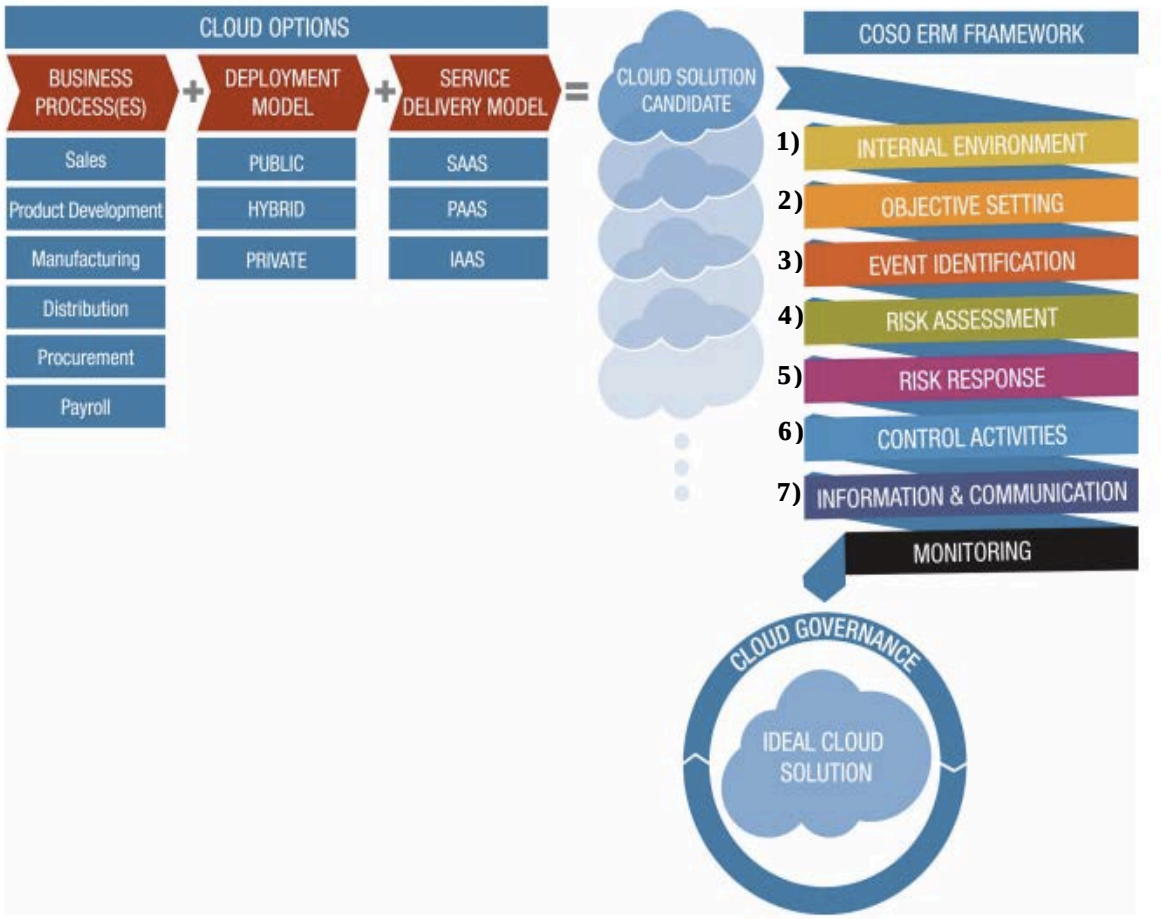

Figure 4: Applying the COSO ERM Framework to Cloud Computing Options
(Crowe Horwath LLP, Chan, Leung, & Pili, 2012)

Applying COSO's ERM framework to the business processes or application domains supported by cloud providers delivers management a more complete view of associated risks, benefits and risk response options. This framework focuses on 1) Internal Environment - how risks and controls are viewed; 2) Objective setting - aligning organization objectives; 3) Event Identification - identifying opportunities or risks; 4) Risk Assessment - determining the impact of risks; 5) Risk Response - mitigating risk; 6) Control Activities - assigning control responsibility (organization or cloud service provider); and 7) Information and Communication - establishing timely and accurate communication flows. Depending on the combination of cloud options (business processes, deployment and service delivery models), risk, security and compliance concerns will vary and should be accounted for in ERM program. "It is a best practice to incorporate cloud governance in the initial stages (when a cloud computing strategy is being defined) before a cloud solution is adopted. For organizations that already have adopted cloud computing without following best ERM practices, it is still prudent to perform a risk assessment and establish cloud

governance" (Crowe Horwath LLP, Chan, Leung, & Pili, 2012). The COSO ERM can be tailored to each unique cloud solution.

With regard to spelling and punctuation, you may use any dialect of English (e.g., British, Canadian, US, etc.) provided this is done consistently. Hyphenation is optional. To ensure suitability for an international audience, please pay attention to the following:

- Write in a straightforward style.
- Try to avoid long or complex sentence structures.
- Briefly define or explain all technical terms that may be unfamiliar to readers.
- Explain all acronyms the first time they are used in your text – e.g., "Digital Library (DL)".
- Explain local references (e.g., not everyone knows all city names in a particular country).
- Be careful with the use of gender-specific pronouns (*he*, *she*) and other gendered words (*chairman*, *manpower*, *man-months*). Use inclusive language that is gender-neutral (e.g., *they*, *s/he*, *chair*, *staff*, *staff-hours*, *person-years*).

ENISA

The European Network and Information Security Agency (ENISA) published a guide to assess the security risks and benefits of using cloud computing. This guide, "Cloud Computing: Benefits, risks and recommendations for information security", reviews technical and legal risks as well as policy and organizational issues (ENISA, 2009). The framework illustrated in Figure 5 continues to demonstrate the overlapping relationships introduced in Figure 1 by incorporating the Business Process/Application dimension from the CobiT framework (Figure 2) and the COSO ERM framework (Figure 4).

The ENISA governance framework is in part based on the broad classes of controls from the ISO 27001/2 and BS25999 standards (ENISA, 2009) and elements of the COSO Internal Control – Integrated Framework. The ENISA framework provides a set of assurance criteria designed to assess the risk of

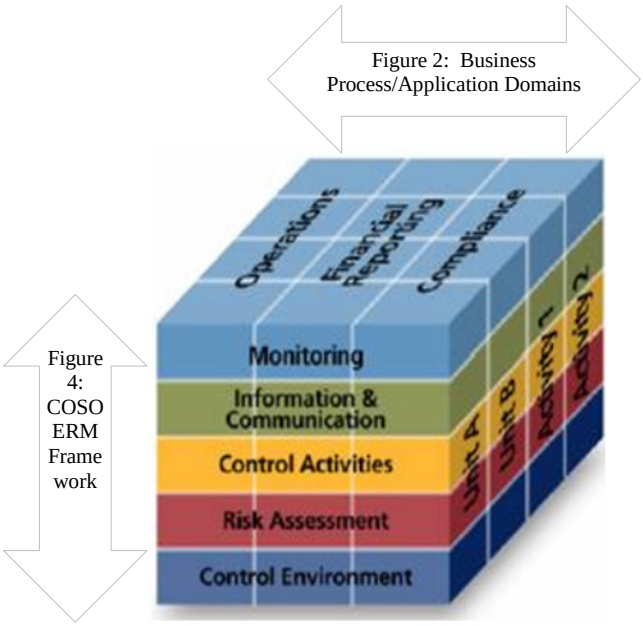

Figure 5: ENISA Governance Framework based on COSO's Internal Control Integrated Framework **(ENISA.europa.eu)**.

adopting cloud services, compare services offered by cloud service providers (CSPs), obtain assurance from CSPs, and reduce the assurance burden on cloud providers. The framework also provides a set of questions designed to provide a minimum baseline which is intended to feed into a more detailed comprehensive framework. This process adaptation is related to personnel and operational security and to the supply-chain assurance. ENISA offers a list of areas that should be included in legal agreements which includes data protection and transfer, confidentiality, intellectual property or limitation of liability (Rebollo, Mellado, & Fernandez-Medina, 2012).

ITIL

The IT Infrastructure Library (ITIL) provides a set of best practices that have become the most widely accepted approach to IT service management in the world. "ITIL advocates that IT services must be aligned to the needs of the business and underpin the core business processes. It provides guidance to organizations on how to use IT as a tool to facilitate business change, transformation and growth" (What is ITIL?, 2012). Furthermore, ITIL provides a common vocabulary (semantics) enabling the discussion of the stages and activities required to build and maintain ITSM systems in a common language (GTSI, 2008). If an organization's processes are defined per the best practices of the ITIL framework, the amount of effort necessary to extend this framework to the cloud will be reduced. "Core IT management disciplines have not changed – just shifted from the IT organization to the cloud service provider, and ITIL is well positioned to help. Nearly all the ITIL disciplines can be used when leveraging services delivered via the cloud" (Bentley, 2010).

ISO 27000/9000

The International Standards Organization (ISO) 27000 series of standards offers cloud risk assessment tools. ISO 27001 is the international best practice standard for an Information Security Management System (ISMS). The proposed "ISO 27017 standard is expected to be a guideline or code of practice recommending relevant information security controls for cloud computing. ISO 27017 standard will recommend, in addition to the information security controls recommended in ISO 27002, cloud-specific security controls" (IT Governance Online, 2012). However, according to Kosutic (2011), currently the following ISO 27001 risk assessment security controls may be successfully applied to cloud computing:

- A.6.2.1: Identify "risks to the organization's information and information processing facilities from business processes involving external parties"
- A.6.2.3: Address security issues in agreements that "cover all relevant security requirements"
- A.10.5.1: Information backup controls
- A.11: Access control

Comprehensive IT governance may also include operational compliance initiatives and standard quality management methodologies based on ISO 9000. "ISO 9000 is a series of international quality standards, the guiding principle of which is the prevention of defects through the planning and application of *best practices* at every stage of business - from design through to installation and servicing" (ISO Center). Relevant to cloud governance, "ISO 9001 provides the definition of the characteristics and associated quality evaluation process to be used when specifying the requirements for and evaluating the quality of software products throughout their life cycle" (ISO 9000).

Integrating Cloud IT Governance Models and Frameworks

It is important to note that there are numerous IT governance models and frameworks, many of which are derived from the respected standards and best practices of the primary IT standards setting bodies as discussed in the previous section. The choice of a particular model or a blend of different aspects of several models is dependent on the organization, personnel, and the maturity and effectiveness of the organization's current IT governance model. The extension to the cloud computing paradigm, therefore, begins with a current IT governance model.

The ITGI identifies five IT governance domains as shown in Figure 6:

1. **Strategic alignment** – IT and business plans are linked to add enterprise value
2. **Value delivery** – IT value proposition delivers promised benefits against strategy
3. **Risk management** – Enterprise risk strategy addressing IT assets, disaster recovery, and continuity of operations. With a move to the cloud, the importance of this dimension is magnified exponentially.
4. **Resource allocation** – Optimal investment, use and allocation of IT resources
5. **Performance management** – Translating strategy into action to achieve goals

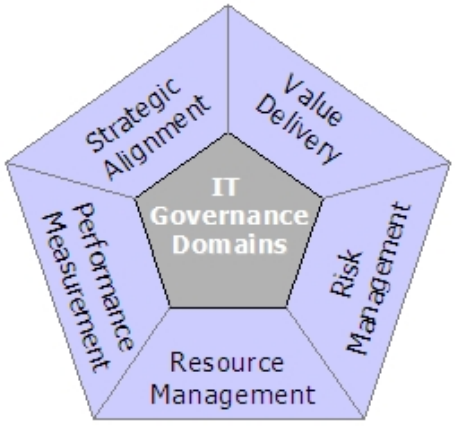

Figure 6: IT Governance Domains *Source: COBIT 4.1 ©1996-2007 IT Governance Institute* (ISACA, 1996-2007) .

Weill & Ross (2004) suggest four IT governance deliverables: business growth, cost effectiveness, asset utilization, and business flexibility/agility. These deliverables help companies align IT initiatives with business priorities. As more businesses include cloud services in their IT initiatives, the governance domains expand to encompass the issues unique to cloud deployment, especially in the area of security.

Extending IT Governance to the Cloud

Because governance is not a one-size fits-all proposition, the scale and structure must consider the enterprise goals, maturity, complexity and culture of the IT organization. Extending governance to the cloud increases the difficulty of effective IT governance. "The new cloud environment is very different from traditional outsourcing and requires a new approach to governance and management" (Dreyfuss, 2009). Moving to the cloud forces the customer to accept the control of the service provider on a number of important issues and areas of the business process (Mangiuc, 2011).

While the adoption of cloud services and resources offer many benefits, it also raises important issues that should be analyzed prior to any migration efforts such as:

- Internal threats
- Horizontal audit compliance
- Performance metrics
- Security
- Accountability and responsibility

Internal threats regarding standards, controls, interfaces, handoffs and integration requirements should be addressed with policies and procedures that clearly depict how all these elements fit together. Horizontal audit compliance tools can show where organizations are vulnerable across functional silos. A horizontal audit compliance framework will provide a view across all business units and combine the information streams. Performance metrics provide a quantifiable assessment of successful cloud resource integration. Detailed Service Level Agreements (SLA) often provide the specific requirements of both the CSP and the client. Measuring performance internally and externally offers insight into areas that have been identified for IT-business alignment and can serve as an early warning system for risk and security. Some organizations may consider increasing security control when moving to the cloud. By leveraging the security information and event management deployment, cloud consumers ensure the successful integration of data from the cloud as well as from its own identity and access management solution. Security as a service (SecaaS) could provide a solution to new or immature organizations with limited funds and/or internal resources. To avoid potential pitfalls of extending governance to the cloud paradigm, organizations should put in place and sustain a practical governance framework to ensure cloud infrastructure and operations are as secure, if not more so, than traditional IT governance approaches.

Achieving accountability in the context of cloud computing requires mechanisms that result in trust and security. The responsibility of successful implementation and enforcement of these mechanisms ultimately remains with the customer. Cloud governance accountability and responsibility may be viewed as follows:

ACCOUNTABILITY	**RESPONSIBILITY**
Preventive Controls	Customer vs. Provider
Detective Controls	Compliance
Procedural Measures	Data Management
Technical Measures	Forensics & Recovery

Accountability

Accountability promotes the implementation of controls where legal requirements, legislation, and policies can be translated into effective data protection. Prospective and proactive accountability is achieved through preventive controls. "Preventive controls for the cloud include risk analysis and decision support tools, policy enforcement, trust assessment, obfuscation techniques, and identity management" (Pearson, 2011). Organizations can employ detective controls to identify privacy or security risks. Effective detective controls for the cloud include auditing, tracking, reporting and monitoring. Contracts, service level agreements, and data flow restrictions are all procedural measures for accountability that begin prior to selecting a CSP. Additionally, technical measures for accountability are used to maintain appropriate separations, enforce policies, and report information accurately. Encryption is an essential technical measure for cloud data security.

Responsibility

Although cloud computing removes some IT responsibilities from the client, governance is not one of them. There is no debate of customer versus service provider responsibility because despite the handoff of certain IT functions, the responsibility of governance still remains at home. Compliance risks will require cloud-based service providers to produce evidence of their own compliance with industry standards and regulatory requirements and perhaps permit audit by the cloud customer (Mangiuc, 2011). Data Management poses data risks for both the cloud customers and providers. The customer must be able to effectively monitor the data handling practices of the provider and in some cases require certification of data processing, security and control activities (Mangiuc, 2011). Forensics and recovery are unique challenges complicated by logistical issues and undetermined ownership responsibilities. Regulations are needed to remove any ambiguity of responsibility in respect to cloud data.

RACI Matrix

The RACI matrix, also known as a responsibility assignment matrix (RAM), can be used to clarify the roles and responsibilities associated with cloud deployment. RACI is an acronym derived from four key responsibility roles:

- Responsible – who is responsible for a task
- Accountable – who will be held accountable for task completion
- Counsel – who will provide the information needed
- Informed – who is dependent of the information

CobiT 5 contains RACI matrices that "suggests stakeholders to be responsible, accountable, consulted, and informed regarding" IT Governance activities (Simonsson, Johnson, & Wijkstrom, 2007). Weill and Ross define IT governance in part as "specifying the decision rights and accountability framework" (Weill & Ross, 2004) which underscores the need for ownership assignment of responsibilities and accountability for IT governance. The cloud environment introduces new and changing roles and responsibilities within the organization and between the organization and the CSP. In the cloud,

ownership no longer refers only to physical access. Governance, compliance, responsibility and accountability are on-line and real-time and require new ownership assignments.

Deconstructing the Cloud

The Cloud Security Alliance (CSA) released the second version of "Security Guidance for Critical Areas of Focus in Cloud" in 2009. A portion of this guide deals with governing in the cloud and more specifically governance and enterprise risk management. The guidelines provided help to identify threats and mitigate vulnerabilities when adopting cloud architecture.

The key is to deconstruct the cloud services and architecture to map a model of compensating security and operational control, risk assessment frameworks, and management frameworks to create compliance standards (Cloud Security Alliance, 2009).

Using the Cloud Computing Service Delivery and Deployment Model presented in Figure 2 (Cloud Security Alliance, 2009), deconstruction begins by assessing each application domain or business process individually and asking the following questions:

1. What is moving to the cloud? (application domain or business process)
2. How will it be delivered? (SaaS, IaaS, PaaS, BPMaaS)
3. How will it be deployed? (Public, private, community/managed or hybrid)

Deconstruction based on this model would result in an isolated cube (for example: the payroll process delivered as SaaS on a public cloud). There are sixteen possible delivery and deployment possibilities for a single application or process (4 delivery models * 4 deployment models).

The next phase of deconstruction will determine the cloud formation by employing the Cloud Cube Model described in Figure 3 (JerichoForum.org). In order to position the isolated cube within this model, it is necessary to determine:

1. Where will the data be located? (internal or external)
2. Who owns the technology, services, and interfaces? (proprietary or open)
3. Are there expectations of collaboration and data sharing? (perimeterised or de-perimeterised)
4. Who is managing the delivery? (insourced or outsourced)

By combining the sixteen delivery and deployment options with the eight cloud formations (see Figure 3) then choosing whether to insource or outsource, the decision to move a single application domain to the cloud results in 256 possible outcomes (16 * 8 * 2), each presenting a set of governance challenges. However, each outcome does not necessarily require unique ERM and Control frameworks (Figures 4 and 5). Many risk management and control objectives will be common to all cloud outcomes while others will be tailored to groups of outcomes with common risk and control objectives. The necessity to develop a customized ERM and/or control framework for a single outcome would be an exception.

Risk Management

Risk is the most important and involved factor in this deconstruction process. Cloud risks introduce additional assessment and management requirements. Figure 7 depicts the hierarchy of the four key enterprise IT risk factors identified by Westerman (2006): Agility, Accuracy, Access, and Availability. "The pyramid provides a map for addressing the complexity of IT risks" (Westerman, 2006). These four factors will now be addressed in the context of the cloud environment.

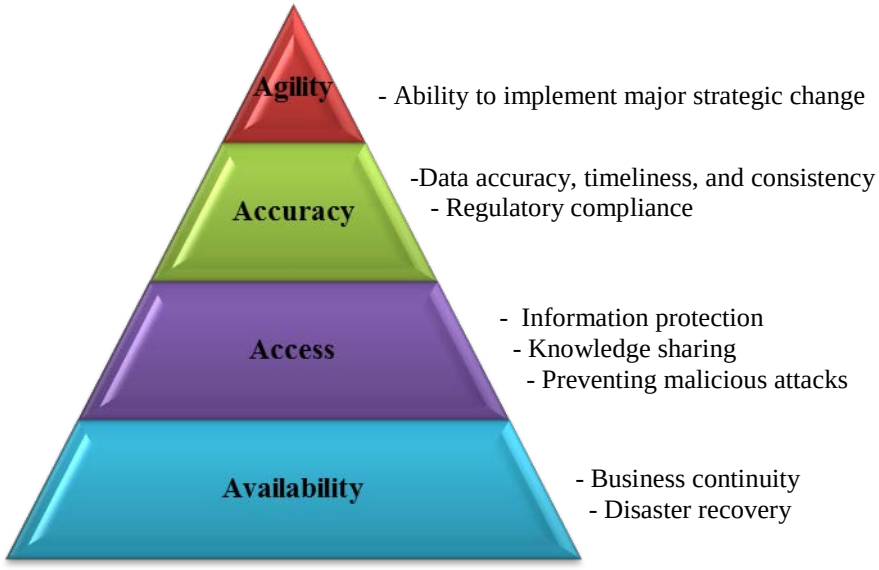

Figure 7: Hierarchy of IT risk factors **(Westerman, 2006)**

Availability - integration management. The cloud environment necessitates the careful design and execution of integration among providers. The architecture at all levels must be designed beforehand and it should clearly indicate the spaces to be filled with cloud services. The integration management of cloud services includes coordinating the interoperability of in-house and cloud services, applications and infrastructure. Additionally, SLAs must contain provisions which address cloud connectivity to ensure critical system availability and continuity during and after cloud deployment.

Access - risk management. Migration to the cloud introduces new and extended areas requiring risk management including data handling, interface management, multi-tenancy, and the security and legal compliance for sensitive data. Many of these risks can be addressed through effective contract designs and comprehensive SLAs. More advanced issues that should be considered in later-stage SLA and contract design may include topics such as optimal risk transfer, security breach reporting, forensics and evidence gathering mechanisms, incident handling, and international differences in relevant regulations including data protection and privacy.

Controls: Authentication, access & encryption. "Cloud computing services can make it difficult to enforce governance policies of service, security or management" (Rose, 2011). Extending the IT function to the cloud complicates IT governance and necessitates a change of approach in sensitive areas such as privacy. Some security professionals believe the focus should be on securing the data, not the systems, and determine who is using the data and how. Data protection measures such as authentication, access control, and encryption guard against degradation of cloud services caused by either action or inaction occurring in-house or in the cloud.

Privacy and security. Privacy issues and regulations make it "imperative for providers to prove to customers that privacy controls are in place and demonstrate ability to prevent, detect and react to security breaches in a timely manner" (Vael, 2010). Cloud computing may result in sensitive data ending up in a "storage system in a country where privacy laws are lax or even nonexistent" (Rose, 2011). Privacy regulations such as the Health and Human Services Health Insurance Portability and Accountability Act (HIPPA) may impede the adoption of the cloud computing paradigm. Although HIPPA and other regulations at the local, national, and international level may currently be seen as roadblocks, proactive government actions such as the formation of the EuroCloud are the initial developments necessary to resolve cross-border issues (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Accuracy – data integrity and regulatory compliance. Accuracy consists of compliance and regulatory issues across both domestic and international borders, which are discussed now.

Compliance (legal, regulatory, and audit). When companies choose to transfer components of their business to the cloud, they are not transferring their obligation for compliance with legal, regulatory and audit requirements. Differing classes of data may be subject to different policies and legal rules. The increasing use of cloud architectures requires a corresponding increase in the need for the "auditability, proper prevention and tracking of fraudulent activities, irregularities and control loopholes in the business processes in the cloud" (Ko, et al., 2011). Third party cloud service providers (CSPs) and their customers are legally distinct enterprises. "However, if the CSP neglects or fails in its responsibilities, it could have legal liability implications for the CSP's customer organization. But if a cloud customer organization fails in its responsibilities, it is less likely there would be any legal implications to the CSP" (Crowe Horwath LLP, Chan, Leung, & Pili, 2012).

- **Trust and transparency of controls.** "Cloud computing requires companies and individuals to transfer some or all control of computing resources to cloud service providers (CSPs)" (Ko, et al., 2011). This transfer raises an acute concern regarding trust. Consumers want to know who has access to their data. Controls for privacy and security can mitigate the risks, however full transparency of these controls is necessary to provide the cloud consumer with the capability to assess and monitor the accountability and auditability of the CSPs. CSPs "must demonstrate [the] existence of effective and robust security controls [that] assure customers their information is properly secured against unauthorized access, change and destruction" (Vael, 2010).
- **ii. Audit controls**. Increased cloud computing usage mandates the need for auditability for the prevention and tracking of fraudulent activities, irregularities and control loopholes which may occur in business processes in the cloud. Cloud frameworks must implement effective audit controls of processes, standards, and compliance methods which not only include business logic and control flows, but also the applications implementing them (Ko, et al., 2011). Effective audit controls insure that the cloud based services are implemented in accordance with recognized policies and audit procedures.
- **iii. Certification.** The certification of CSPs provides assurance to the customers that the providers are meeting regulatory requirements and industry standards. Certification provides "independent assurance from third-party audits and/or service auditor reports" (Vael, 2010) that providers are adhering to these requirements and standards. The CSA Certificate of Cloud Security Knowledge (CCSK) and the CSA Security, Trust & Assurance Registry (STAR) are offer by the Cloud Security Alliance (CSA) to provide assurance of compliance with cloud security competency standards and a registry of CSPs that are able to document their compliance with CSA best practices (cloudsecurityalliance.org). MSPAlliance is an international association of cloud and managed service providers. The MSP/Cloud Certification, the Unified Certification Standard for Cloud and Managed Service Providers (UCS) requires applicants to submit to a comprehensive audit and onsite facilities inspection (MSPAlliance.com). TRUSTe provides cloud data privacy certification to ensure CSP practices, technology and polices meet or exceed customer data security standards (TRUSTe.com). These and other CSP certifications address standards issues unique to the cloud industry.

International regulation, policy and transborder information flows. A healthy governance infrastructure must frame the challenges of governance appropriately. Cloud governance issues transcend jurisdictions. International regulations and policies should encompass the "dynamic, adaptive and complex system of systems that should be viewed as an organic whole, including diverse people, technologies, rules and relationships" (Johnston, 2010). Cloud deployment may include overlapping dimensions that are regulated by multiple sovereignties with interactions that fall outside the familiar jurisdictions of IT governance. IT governance in the cloud is further complicated by the difficulty of CSPs to achieve compliance across geographic boundaries. As dataflow becomes global and dynamic, complying with legislation becomes difficult and complex (Pearson, 2011). Location matters in trans-border information flow especially in determining which laws apply and which courts have jurisdiction. The pre-cloud notions about residency and ownership of data and information have been altered. National and international regulatory agencies are beginning to address these issues and some progress has been made as evidenced by the US-EU Safe harbor laws (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). "Organizations are still responsible for their information even if it's stored elsewhere (in this case, in the

cloud). ISO 15489 (the international standard for records management) defines records as being authentic, reliable and usable and possessing integrity" (Ferguson-Boucher, 2011). Information governance policies and procedures must provide a clear understanding of who is responsible for what. Records management and data mapping standards should contain particular references to data protection and privacy as discussed in the previous section.

Agility - corporate cultural impact. The acceptance of cloud computing is evidenced by the growth of CSPs. The decision to outsource and to engage a CSP to deliver all or part of the IT services will inevitably have a corporate cultural impact. Within the corporate culture, IT has been viewed as a costly utility that is necessary but often unwelcome. The shift to emerging cloud computing alternatives can change the role of IT from a "necessary evil" to a strategically aligned tool not only achieving cost reduction but becoming a driver of innovation and contributing business value. Cloud computing adoption also requires organizational changes where fewer IT personnel are needed in the areas of infrastructure management, technology deployment, application development, and maintenance. This staff reduction could affect the morale and dedication of the remaining IT staff members.

IT CLOUD GOVERNANCE DIAL

As a result of the deconstruction process, the organization's IT governance framework will effectively extend to the cloud computing environment. This systematic approach functions to maintain focus on the five IT governance domains while producing the associated deliverables as they apply to cloud adoption. The processes/components can be viewed as six concentric dials as shown in Figure 8:

1. Process – What is moving to the cloud?
2. Delivery – How will it be delivered (SaaS, PaaS, IaaS, or BPMaaS)?
3. Deployment – How will it be deployed (Public, Private, Hybrid, Managed/Community)?
4. Cloud Formation – Internal/External, Proprietary/Open, Parameterized/De-parameterized, Insourced/Outsourced
5. ERM – What unique risk factors arise from steps 1-4?
6. Control – What are the control modifications necessary for this cloud solution?

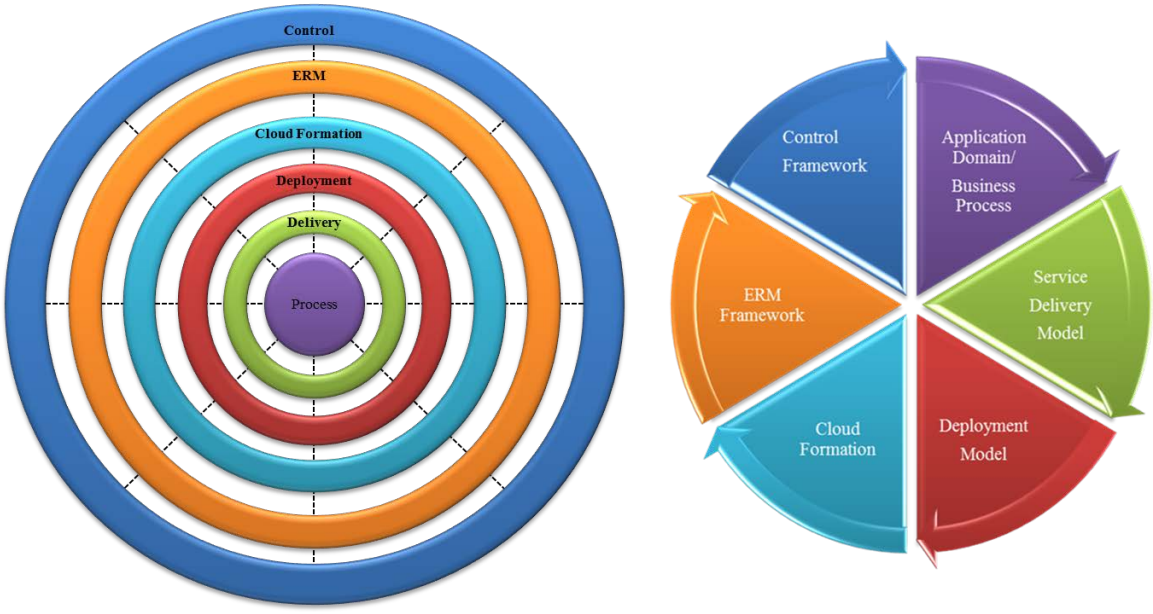

Figure 8: Cloud Governance Dial

The appropriate categories on each dial are aligned to produce the applicable governance framework. Modifications to the existing IT governance framework should address the specific changes required to achieve effective governance of the proposed cloud solution. Aligning the six dials for each (1)

application/process, (2) delivery model, (3) deployment model, (4) cloud formation, (5) ERM framework, and (6) control framework ascertains the critical to additions to the IT governance framework while addressing the IT governance domain objectives (Figure 6). The Cloud Governance Dial allows the organization to align the cloud solution with stated business values and deliver that added value through optimal resource allocation and performance management. The dialed solution can be further evaluated to define the related deliverables to achieve business growth, cost effectiveness, asset utilization, and business flexibility/agility. These factors specify the ERM and control framework adjustments necessary to reduce or eliminate the cloud risk issues arising with each cloud solution.

Conclusions

Enterprises must develop a clear governance strategy and management plan to obtain the most benefit from their cloud initiatives. The plans should set the direction and objectives for cloud computing and exploit the opportunity to fully align IT with the goals of the enterprise and add value to the organization. Cloud computing governance is critical to manage risk, adapt effectively, ensure continuity, and communicate objectives. Standards and good practices can help achieve cloud business goals while addressing risk considerations and responsibilities. Controlling for risk is perhaps the major consideration of moving to cloud computing. We have built upon several robust risk management, cloud deployment, and IT governance frameworks to create a comprehensive risk assessment IT governance/management and management framework for distinctive cloud solutions.

The traditional IT Governance frameworks (COSO, CobiT, ENISA, ITIL, and ISO) establish a governance foundation which is not materially altered by cloud implementations. Additional considerations proffered by Weill and Ross, ITGI, and others have helped to refine the approach. The IT Cloud Governance Dial, which is presented in this paper identifies the necessary steps for implementing governance for a cloud solution. The alignment of the six dials determines the IT Cloud Governance model that is specifically designed to not only meet IT Governance goals, but also achieves alignment with corporate governance. As with the cloud computing environment, cloud governance is in its infancy. The evolution of the cloud governance model will continue as the environment becomes more tested and stable.

REFERENCES

Bentley, Y. (2010, July 31). *Cloud computing: Is ITIL still relevant?* Retrieved from hp.com: http://h30499.www3.hp.com/t5/IT-Service-Management-Blog/Cloud-computing-Is-ITIL-still-relevant/ba-p/2410316

Cloud Security Alliance. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.*

cloudsecurityalliance.org. (n.d.). Retrieved from Cloud Security Alliance: https://cloudsecurityalliance.org/

Cole, B. (2012, April 23). *ISACA: Update to CobiT 5 governance framework maximizes IT assets.* Retrieved from SearchCompliance: ISACA-Update-to-COBIT-5-governance-framework-maximizes-IT-assets

Crowe Horwath LLP, Chan, W., Leung, E., & Pili, H. (2012). *Enterprise Risk Management for Cloud Computing (COSO).* Committee of Sponsoring Organizations of the Treadway Commission.

Deloitte. (2011). *Deloitte Cloud Computing Risk Intelligence Map.* ISACA.

Dreyfuss, C. (2009, August 31). Cloud-Enabled Outsourcing: New Ideas for Effective Governance and Management. *Retrieved from Gartner database.*

ENISA. (2009). *Cloud Computing Information Assurance Framework.*

ENISA. (2009). *Cloud Computing: Benefits, risks and recommendations for information security.*

ENISA.europa.eu. (n.d.). Retrieved from European Network and Information Security Agency: http://www.enisa.europa.eu/activities/risk-management/current-risk/business-process-integration/governance/ics

EuroCloud.org. (n.d.). Retrieved from EuroCloud: http://www.eurocloud.org/

Ferguson-Boucher, K. (2011, Nov. - Dec.). Cloud Computing: A Records and Information Management Perspective. *Security & Privacy, IEE, 9*(6), 63-66. doi:10.1109/MSP.2011.159

Fingar, P. (2010, April). *Extreme Competition*. Retrieved from BPTrends.com: http://bptrends.com/publicationfiles/EIGHT%2004-10-COL-EXT%20COMPETITION-Enterprise%20as%20Svc-Fingar-final1.pdf

Gartner. (2010). *Practical Governance.* Retrieved from Gartner database.

GTSI. (2008). *ITIL Overview: A focused approach to innovation and continuous improvement.*

Haughey, D. (n.d.). *The Project Management Body of Knowledge*. Retrieved from ProjectSmart: http://www.projectsmart.co.uk/pmbok.html

ISACA. (1996-2007). *COBIT 4.1.* IT Governance Institute.

ISACA.org. (n.d.). Retrieved from ISACA: https://www.isaca.org/Pages/default.aspx

ISO 9000. (n.d.). Retrieved from IT Governance Network: http://www.itgovernance.com/iso9000.htm

ISO Center. (n.d.). *What is ISO 9000?* Retrieved from ISOCenter.com: www.isocenter.com/9000/WHATIS.html

IT Governance Online. (2012, June 12). Retrieved from ISO 27017 Security in Cloud Computing: http://www.itgovernanceonline.com/it-governance/information-security/iso-27017-security-in-cloud-computing/

JerichoForum.org. (n.d.). Retrieved from The Open Group Jericho Forum: http://www.opengroup.org/getinvolved/forums/jericho

Johnston, E. (2010, December). Governance Infrastructures in 2020. *Public Administration Review, 70*(s1), s122-s128. doi:10.1111/j.1540-6210.2010.02254.x

Ko, R., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). *TrustCloud: A Framework for Accountability and Trust in Cloud Computing.* Washington DC, USA: IEEE ICFP 2011.

Kosutic, D. (2011, May 30). *Cloud computing and ISO 27001 / BS 25999*. Retrieved from blog.iso27001standard.com: http://blog.iso27001standard.com/2011/05/30/cloud-computing-and-iso-27001-bs-25999/

Mangiuc, D. (2011). Enterprise 2.0 - Is the Market Ready? *Accounting and Management Information Systems, 10*(4), 516-534.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud Computing - The business perspective. *Decision Support Systems, 51*, 176-189.

MSPAlliance.com. (n.d.). Retrieved from MSPAlliance Cloud Certification: http://www.mspalliance.com/ucs/

Nguyen, B. (2010, November). *A comparison of the business and technical drivers for ISO 27001, ISO 27002, CobiT and ITIL*. Retrieved from trongbang86.blogspot.com: http://trongbang86.blogspot.com/2010/11/comparison-of-business-and-technical.html

opengroup.org. (n.d.). Retrieved from The Open Group Jericho Forum: http://www.opengroup.org/getinvolved/forums/jericho

Pearson, S. (2011, July-Aug.). Toward Accountability in the Cloud. *Internet Computing, IEEE, 15*(4), 64-69. doi:10.1109/MIC.2011.98

Rebollo, O., Mellado, D., & Fernandez-Medina, E. (2012). A Systematic Review of Information Security Goverance Frameworks in the Cloud Computing Environment. *Journal of Universal Computer Science, 18*(6), 798-815.

Rose, C. (2011). A Break In The Cloud? The Reality of Cloud Computing. *International Journal of Management and Information Systems, 15*(4), 59-63.

Simonsson, M., Johnson, P., & Wijkstrom, H. (2007). Model-Based IT Governance Maturity Assessments with COBIT.

TRUSTe.com. (n.d.). Retrieved from TRUSTe: http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-cloud

Vael, M. (2010, May). *Across Cloud Computing governance and risks May 2010 - ISACA.* Retrieved from isaca.org: http://www.isaca.org/Groups/Professional-English/information-security-

management/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

Weill, P., & Ross, J. W. (2004). IT Governance on One Page. *MIT Sloan Shcool of Management*.

Weill, P., & Ross, J. W. (2004). *IT Governance: How top performers manage IT decision rights for superior results*. Boston, Massachusetts: Harvard Business School Publishing.

Westerman, G. (2006, April). The IT Risk Pyramid:Where to Start with Risk Management. *Center for Information Systems Research, Sloan School of Management, V*(1D).

What is ITIL? (2012, June 30). Retrieved from ITIL Offical Site: http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

Wikipedia. (n.d.). *Basel III*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Basel_III

Wikipedia. (n.d.). *Payment Card Industry Data Security Standard*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Wikipedia. (n.d.). *Prince2*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/PRINCE2

Wikipedia. (n.d.). *Sarbanes-Oxley Act*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

Wikipedia. (n.d.). *The Open Group Architecture Framework*. Retrieved from Wikipedia.org: http://en.wikipedia.org/wiki/The_Open_Group_Architecture_Framework

Wikipedia.com International Safe Harbor Privacy Principles. (n.d.). Retrieved from International Safe Harbor Privacy Principles: http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles