IMPACT OF CLOUD COMPUTING ON IT GOVERNANCE

Declan McGrath

EMC²

Overview

Cloud Computing represents a major shift in Information Technology (IT) architecture, altering the way services are sourced and delivered. The pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT Governance. The purpose of this research is to understand the impact of Cloud Computing on ITIL and to answer the following: *What is the Impact of Cloud Computing on IT Governance?* The literature review examined both the concept of Cloud Computing and IT Governance with a specific focus on ITIL and was combined with a review of current thinking in this field. The basis for this research was a single case study, where a number of interviews were conducted with IT Managers in Company A. Using the outcomes of these interviews and having met the three objectives set out in the report a Cloud Readiness Assessment was created and performed on a Cloud Service Provider.

The research found that when the company was selecting a Cloud Solution its focus was outwards at the Cloud Solution as opposed to inwards at the company and its IT Governance framework. As a result, a number of gaps in the Company's IT Governance Framework were identified which present various levels of risk to the business. Through this research and the use of the Cloud Readiness Assessment, the Company is now in a better position to align the Cloud Service to the IT Governance framework and mitigate future risks to the business.

Please Note: This article is an abridged version of the original research topic, findings, and conclusion.

Table of Contents

Table of Figures

Abbreviations

ASP – Application Service Provider

CapEx – Capital Expense

CEO – Chief Executive Officer

CFO – Chief Financial Officer

CIO – Chief Information Officer

CMDB – Content Management Database

CSP – Cloud Service Provide

DaaS – Data as a Service

DBaaS – Database as a Service

FDA – Federal Drug Authority

IaaS – Infrastructure as a Service

IMaaS – Identity as a Service

ISACA – Information Systems Audit and Control Association

ISO – International Standards Organisation

IT – Information Technology

ITIL – Information Technology Infrastructure Library

KPI – Key Performance Indicator

NIST – National Institute of Standards and Technology

OpEx – Operational Expense

ROI – Return on Investment

SaaS – Software as a Service

SCM – Service Catalogue Management

SDP – Service Design Package

SLA – Service Level Agreement

SLM – Service Level Management

SOC – Service Organization Control

TCO – Total Cost of Ownership

VPN – Virtual Private Network

WWW – World Wide Web

XaaS – X as a Service

Chapter 1: Introduction

1.0 Introduction

Cloud computing is causing a major shift in Information Technology (IT) architecture, altering the way services are sourced and delivered. Cloud computing represents a growing evolution in IT in which core IT services are being sliced and diced across many providers (Steinberg & Clarke, 2010). The recent global economic downturn has increased pressure on organisations to improve efficiencies and cut costs by using collaborative solutions and real time information exchange.

The constant evolution of IT has helped organisations automate and innovate thus providing a competitive advantage in the global market place. Early adoption of cloud services can provide these organisations with an opportunity to transform their business model and gain advantage on competitors. While cost reduction is one of the benefits there are a number of others, such as rapid deployment of services to enable the organisation to capitalise on opportunities that may otherwise be lost (KPMG, 2011). Organisations can then concentrate on their core competencies while cloud providers focus on running their IT infrastructure.

A move to the cloud, however, requires a well-planned strategy as there are many business and technical constraints to be mitigated. IT Governance and regulation are required to clear any doubts with regard to security and management of the organisation's data. IT Governance is part of a wider Corporate Governance activity, but the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT Governance. Management and security of data are common concerns for organisations and any organisation wishing to move their services to the cloud will ask, "How secure is my data and service?" The challenge for organisations when adopting cloud services is to understand the maturity and robustness of their IT Governance framework.

1.1 Research Question

Cloud technology is not a new technology but a new way of delivering computer resources, while Information Technology Infrastructure Library (ITIL) is the most widely accepted framework for the management and delivery of Information Technologies. Kim (2003) suggests ITIL is the best practices for an organization's IT processes. Company A, who use ITIL as their IT Governance framework, have begun to deploy Cloud Services as a means of meeting new customer and business demands.

The purpose of this research is to understand the impact of Cloud Computing on ITIL and to answer the following:

What is the impact of cloud computing on IT Governance (ITIL)?

This will be met through the following objectives.

What considerations are taken into account by companies when they move their data or client's data to a Cloud Service Provider (CSP)?

When considering cloud service solutions, organisations need to have a clear understanding of the underlying drivers as there can be a number of reasons for this, such as cost reduction, flexibility, or IT not meeting the business needs. This objective has been included in the research to get an understanding as to why Company A decided to implement a cloud service solution above their traditional IT organisation. It is very important to understand this because careful consideration must be given when adopting cloud solutions and organisations must ensure it reflects their strategic direction and is aligned to their business needs.

What type of Cloud Readiness Assessment, if any, are taken by companies?

Once a cloud service solution has been adopted, the organisation must ensure they are in a position to integrate the new solution. The rationale behind this objective is to understand what type of assessment a company uses when adopting a cloud service. There is a gap in the literature whereby an assessment would allow you to quickly assess a cloud service and identify how it would align to a company's IT Governance framework.

How do you match your IT Governance framework to the IT Governance framework of a CSP?

Once the strategy has been decided and the assessment completed, an organisation needs to understand how the service will be managed on an ongoing basis. This objective has been included in the research to get a better understanding of Company A's IT Governance framework and to verify if there are any gaps or potential changes in their current processes. It is also important that the CSP ensures they meet the security, availability, or regulatory requirements that are required by the organisation.

Having met each of these objectives it is envisaged that the project will:

Create a Cloud Readiness Assessment document which will prepare a business for a move to a cloud service provider and assess its suitability.

The basis for the assessment document is to allow management to assess each cloud service offering and its suitability for the business. They must ensure that it is aligned with the strategy and business needs of the organisation.

Align Company A's IT Governance Framework to the cloud service solution that ensures there are no gaps which could potentially pose a risk to the Business.

Once the cloud offering has been decided on, it will then require alignment with Company A's IT governance framework.

Chapter 2: Literature Review

2.0 Cloud Computing

The term “Cloud” was borrowed from telephony. Virtual Private Network (VPN) services for Data Communications offered guaranteed bandwidth at a lower cost by balancing switch traffic, thus utilizing network bandwidth more efficiently. It was impossible to predict in advance which paths the traffic would be routed over so the term “Telecom Cloud” was used to describe this type of networking (Giordanelli & Mastroianni, 2010).

The concept of “Cloud Computing” dates back to John McCarthy’s MIT centennial speech in 1961 and suggested at the time that computers may be organised as a public utility just like the telephone system (van der Aalst, 2010). In the mid 90’s, the term “Grid” was coined to describe technologies that would enable customers to obtain computing power on demand (Foster et al, 2008). It is analogous with a power grid in which many power plants supply energy that customers can draw at will (Kaiserswerth et al, 2012). Salesforce.com was established in 1999 and provided “on demand” computer services, or Software as a Service (SaaS), to their customers (Giordanelli & Mastroianni, 2010).

In 2001, IBM introduced the notion of computer systems that can manage themselves—Autonomic Computing—thus leading to concepts like self-configuration and self-optimization of complex IT systems (Kephart & Chess, 2003). In 2007, IBM, Google, and six Universities embarked on a large scale research project into cloud computing, thus providing a launch pad for University students into this area (Lohr, 2007).

Cloud computing is regarded as a relatively immature service offering and as a result, clear understandings of what it is, outside of general definitions, does not yet exist (ISACA, 2012).

2.1 Definition: Cloud Computing

Vaquero et al (2009) suggest a cloud is a large pool of easily usable and accessible virtualized resources. These resources can be dynamically re-configured to adjust to the variable load allowing for optimal resource utilization. Similarly, Pritzker (2009) suggests the cloud is a vast virtualized resource pool with on-demand resource allocation which can be charged back like a service utility. Cloud applications can then be delivered over the Internet as services and supported by hardware and software systems in data centres which provide those services (Armbrust et al, 2010). The expectation is that the service will be virtualized or hidden from the user and taken care of by systems and/or professionals that are somewhere else (Berger, 2009).

Providing a more detailed definition the National Institute of Standards and Technology (NIST) describes:

"*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell & Grance, 2011, p. 2).

This is a commonly referenced definition (Chen, Paxon, & Katz, 2010, Khajaeh-Hosseini, Sommerville, & Sriram, 2010, Al Morsy, Grundy, & Muller, 2010) and includes characteristics, service models and deployment models for cloud computing.

Figure 1 provides a visual summary of the NIST definition of Cloud Computing.

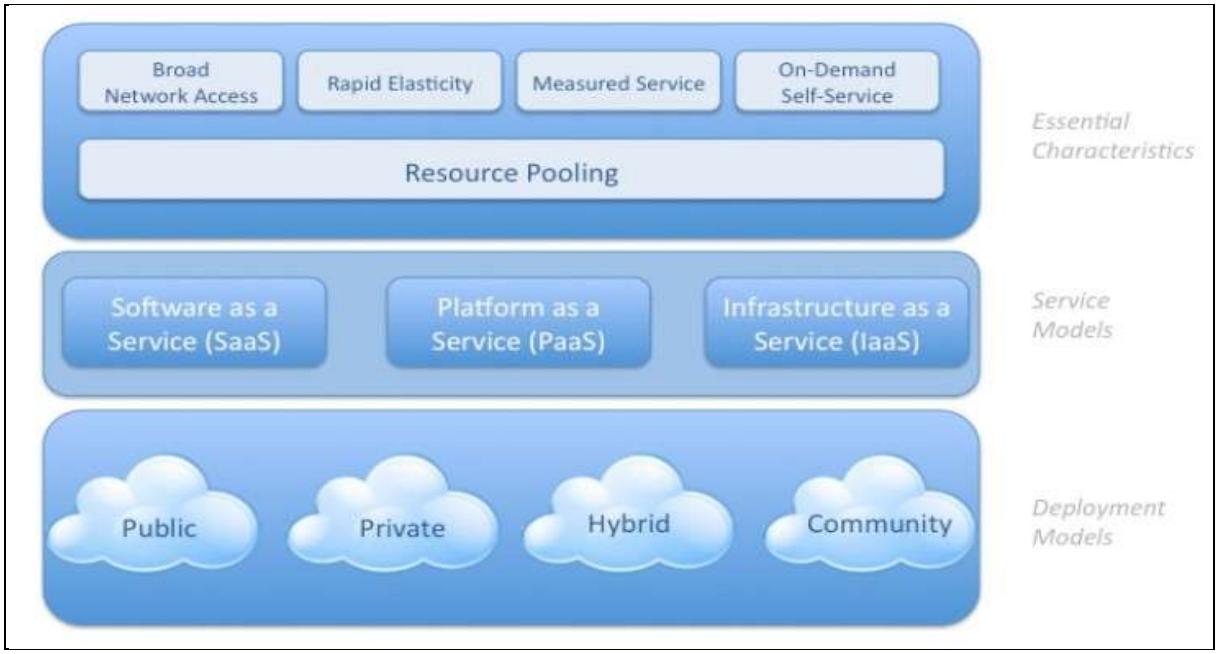

Figure 1: NIST Visual Model of Cloud Computing Definition

Source: Cloud Security Alliance, 2009

2.1.1 Characteristics

The NIST cloud model is composed of five essential characteristics:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client.

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model which can be dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released to scale rapidly outward and inward commensurate with demand.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

2.1.2 Service Models

The NIST Cloud Computing model outlines three layers or service models

Infrastructure as a Service (IaaS): Refers to the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources.

Software as a Service (SaaS): Refers to the capability provided to the consumer to use the provider's applications running on a cloud infrastructure.

Platform as a Service (PaaS): Refers to the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

Service models and their interaction between the internal IT organisation and the CSP are outlined in Figure 2.

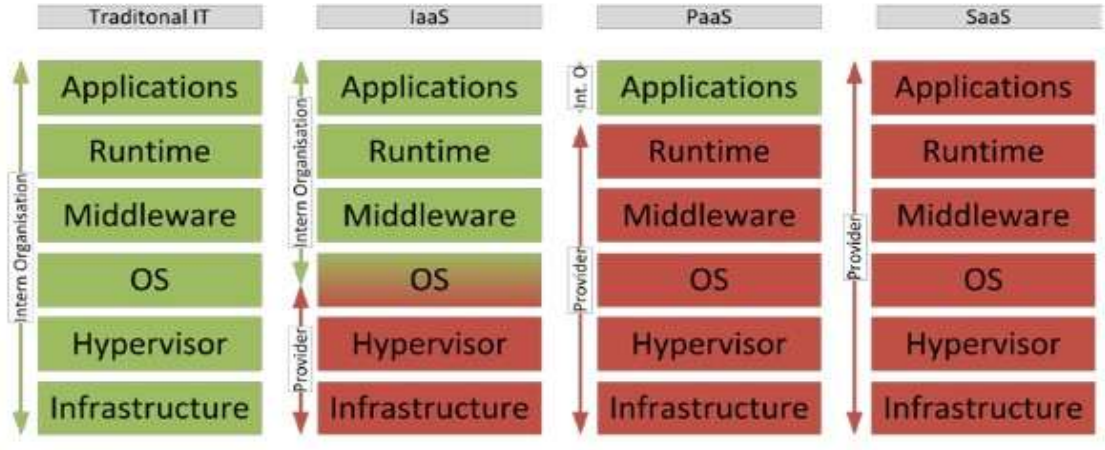

Figure 2: Service Models and Internal IT

Source: Kaiserswerth et al, 2012

2.1.3 Deployment Models

In the NIST Cloud Computing model, services can be deployed using one of the following core models:

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.

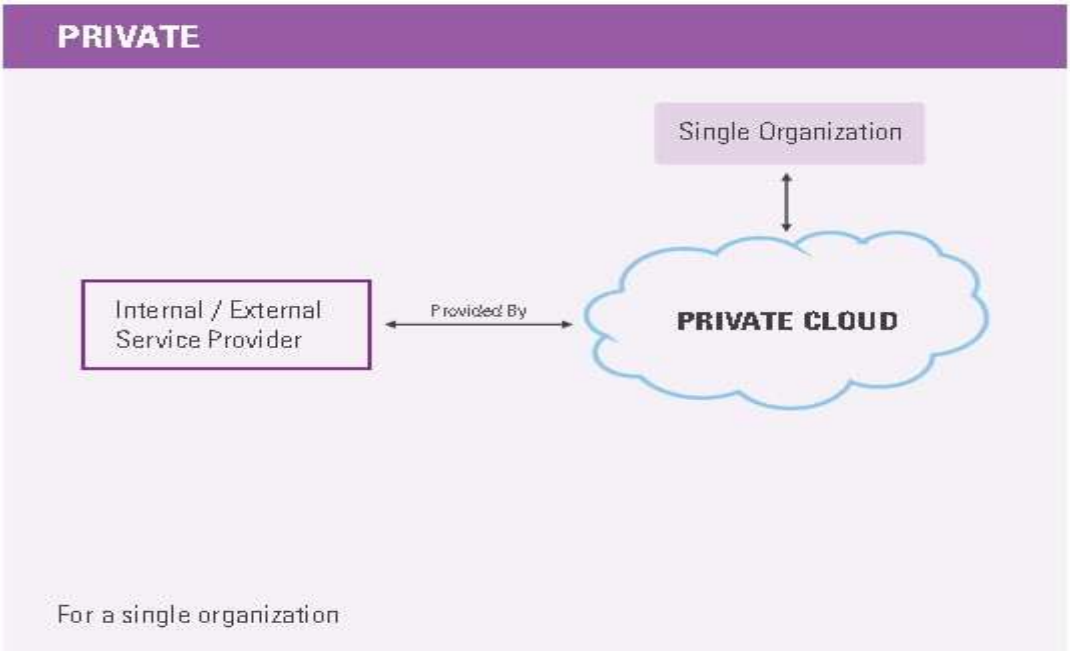

Figure 3: Private Cloud

Source: KPMG, 2011

Public cloud: The cloud infrastructure is provisioned for open use by the general public, government, or large industrial groups.

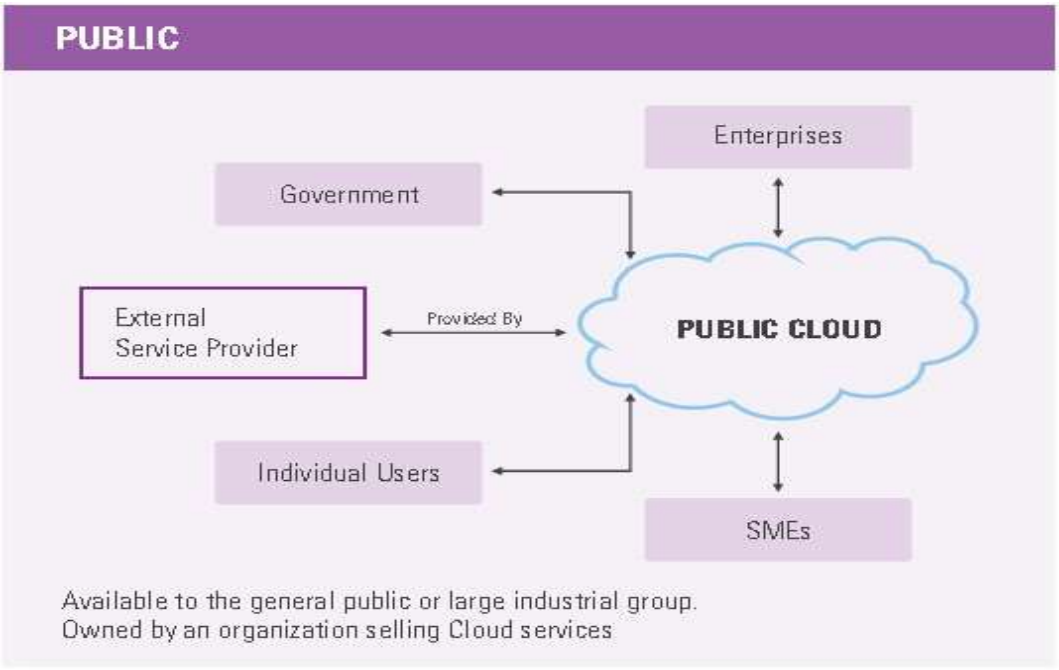

Figure 4: Public Cloud

Source: KPMG, 2011

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.

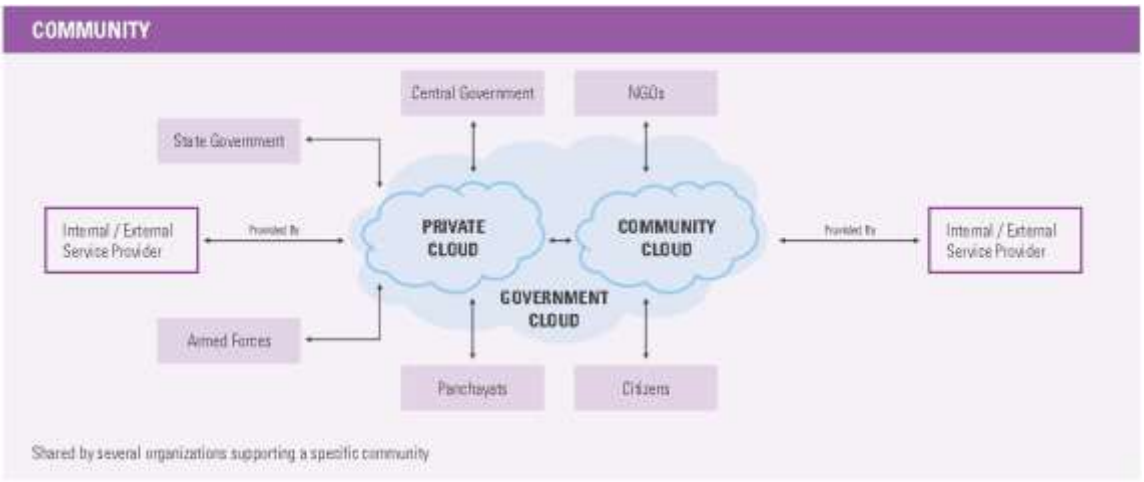

Figure 5: Community Cloud

Source: KPMG, 2011

***Hybrid cloud*:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures listed above.

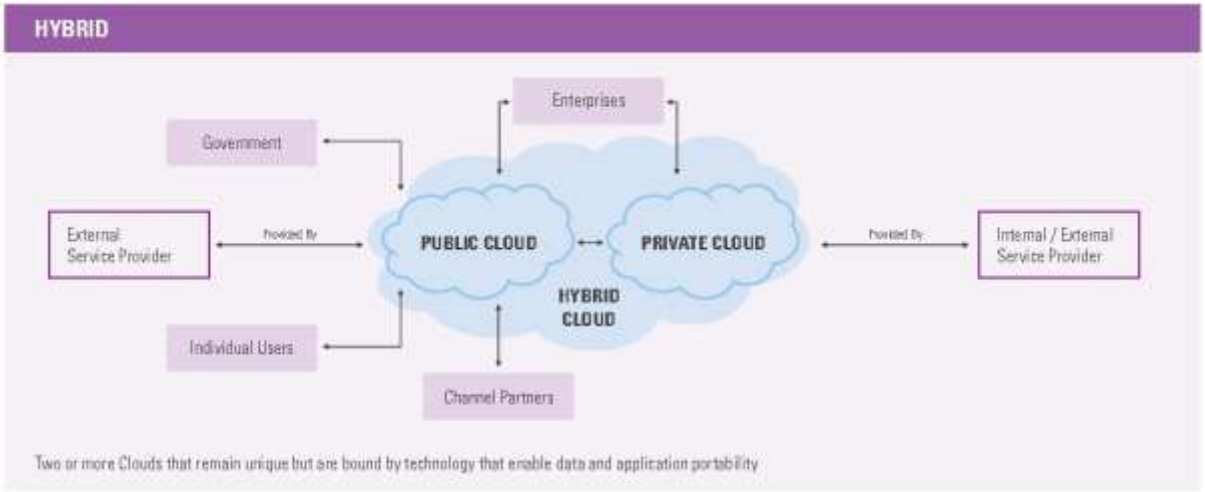

Figure 6: Hybrid Cloud

Source: KPMG, 2011

2.2 IT Governance

Information Technology (IT) Governance is not an isolated discipline of activity; it is part of wider Corporate Governance activity. Governance developments have primarily been driven by the need for the transparency of enterprise risks and the protection of shareholder value. IT is fundamental for managing enterprise resources as many organisations now engage in business on global-scale systems and network downtime has become far too costly for any enterprise to afford. The pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT Governance to ensure minimum disruption to service and mitigate against risks to the business. (Van Grembergen et al (2004b), IT Governance Institute (2003))

2.2.1 Definition

Stakeholders in a business have a number of expectations which include sustaining the current business or growing new business. It is suggested that these can only be achieved with adequate governance of the enterprise IT infrastructure (IT Governance Institute, 2003). Similarly Wessels & Van Loggerenberg (2006) suggests that the aim of IT Governance is to align business and IT strategies more effectively and efficiently. IT Governance is the responsibility of the Board of Directors and executive management. It is viewed as an integral part of Enterprise Governance which consists of the leadership, organizational structures, and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives (IT Governance Institute, 2003). Van Grembergen &

De Haes (2004a, p. 1), in their definition of IT Governance discuss the idea of the fusion of business and IT and suggest:

"*IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT".*

Patel (2002) adds an extra dimension to the definition of IT Governance by including product and service quality. He suggested that the main aim of IT Governance is to contribute to business activity in terms of lower costs, satisfied customers, and better quality products and services provided by a company. Furthermore, Patel (2002) also argues that IT Governance will improve organizational accountability, resulting in better return on investments. The benefits of good IT Governance not only reduce the cost and damage caused by IT failures but also engenders greater trust, teamwork, and confidence in the use of IT itself and the people trusted with IT services. (The National Computer Center, 2005).

2.2.2 IT Governance Lifecycle

Ultimately, IT governance is concerned with IT's delivery of value to the business and the mitigation of IT risks. The first is driven by strategic alignment to the business and the second is driven by embedding accountability into the enterprise. For success, it is essential that there are adequate resources available which are measured to ensure satisfactory results are obtained. IT governance is a continuous life cycle with five main focus areas which are all driven by stakeholder value. These focus areas include IT value delivery and risk management which are considered outcomes, whilst IT strategic alignment, performance measurement and IT resource management are all considered drivers (IT Governance Institute, 2003).

An overview of the IT Governance Lifecycle is shown in Figure 7.

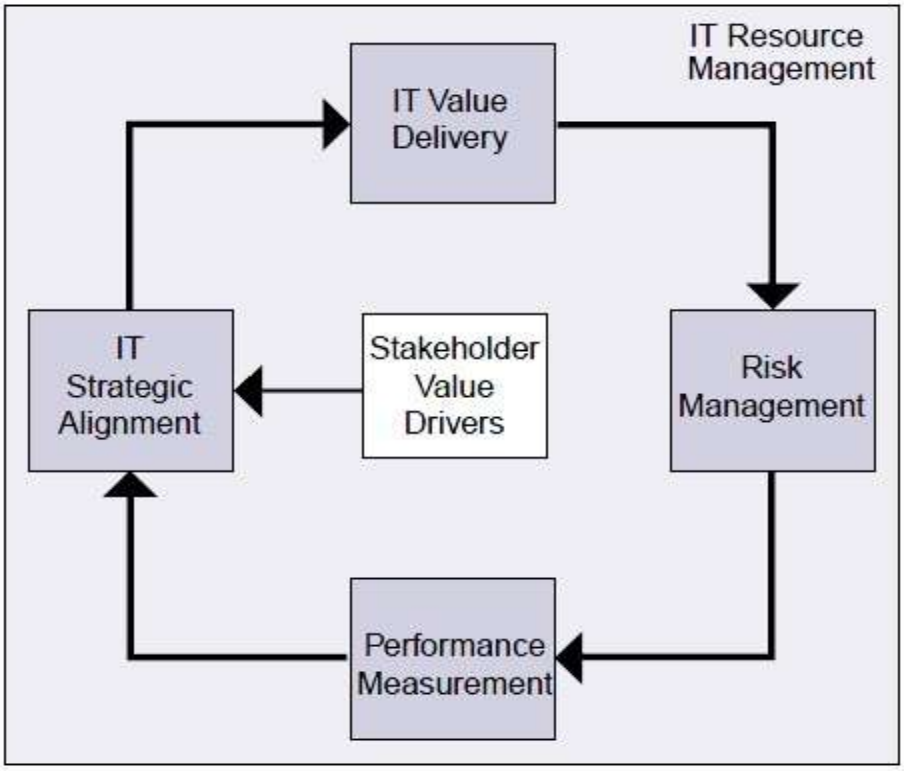

Figure 7: IT Governance Lifecycle

Source: IT Governance Institute, 2003

The lifecycle usually starts with strategic direction of IT and its alignment throughout the enterprise. When delivering value, confirmation is required that the IT/Business organisation is designed to drive maximum business value from IT and assess the return on investment.

Risk management is crucial and IT/Business must ascertain that processes are in place to ensure that risks have been adequately managed.

Along with the contribution of IT to the business, strategy needs to be monitored at regular intervals and the results measured, reported, and acted upon. IT resource management is essential for success and encompasses the entire lifecycle. It is imperative that adequate IT capability and infrastructure is available to support current and expected future IT requirements.

2.3 Information Technology Infrastructure Library (ITIL)

ITIL, described as the best practices for an organization's IT processes, is the most widely accepted IT Governance framework for the management and delivery of IT (Kim, 2003). The ITIL framework was originally developed by the UK Government and consists of a set of best practices that is collected and updated by a wide range of practitioners (Wessels & van Loggerenberg, 2006). Kim (2003) describes the ITIL framework as a 'process-based approach to IT activity', and suggests that ITIL is not focused on technology, but rather

based on processes critical to organizations. The ITIL framework defines a set of best practices for these processes and as a result, organizations can mature their best practices without regard to specific technologies which are adopted.

However, limitations of ITIL include the development of quality management services, failure to address a software development life cycle, and quality issues relating to operational systems (Anthes, 2004).

2.3.1 ITIL Service Lifecycle

The ITIL Service Lifecycle is similar to the IT Governance lifecycle and all service solutions and activities should be driven by business needs and requirements. The lifecycle is initiated by a change in requirements in the business (Cartlidge, et al., 2007). Each volume of the core is represented in the Service Lifecycle. Service Design, Service Transition, and Service Operation are progressive phases of the lifecycle that represent change and transformation. Service Strategy represents policies and objectives while Continuous Process Improvement represents learning and improvement. The ITIL service lifecycle is outlined in Figure 8.

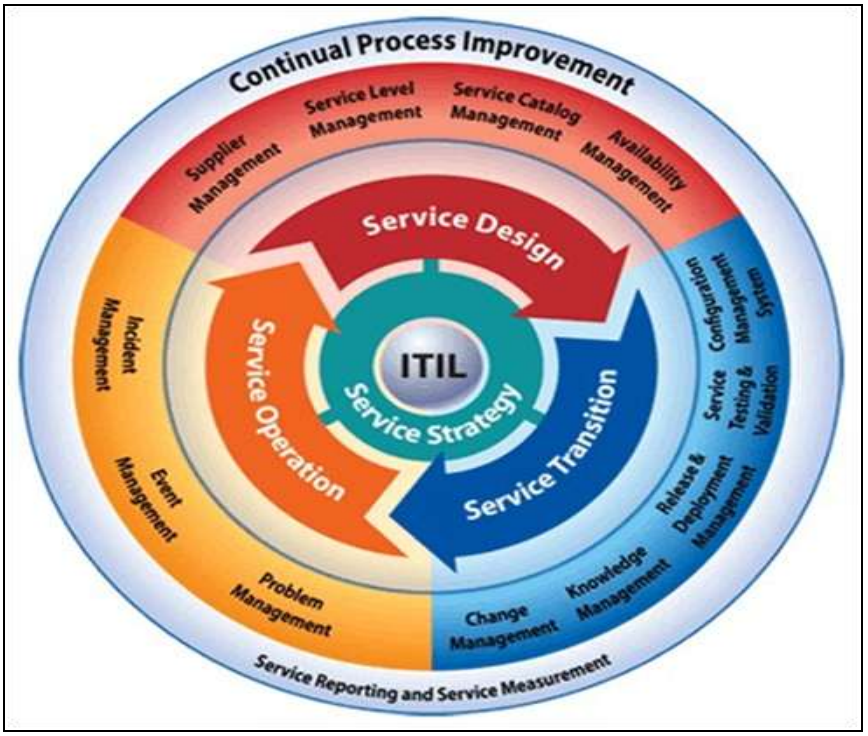

Figure 8: ITIL Service Lifecycle

Source: http://www.hci-itil.com, 2013

Long (2008) describes the different aspects of the ITIL Service Lifecycle which includes Service Strategy, Service Design, Service Transition, Service Operation, and Continual Process Improvement.

- Service Strategy defines an IT organisation's high level approach to providing services. Each organisation must also understand how it will support these services.
- Service Design is a stage in the service lifecycle in which a new or modified service is developed or made ready for the service transition stage.
- Service Transition readies a new or changed service for operation. Prior to moving a service into operation there may be a period of testing and validation to ensure sufficient quality of service.
- In the Service Operation stage, the service which has been developed or modified is now available for IT end users. The service is now monitored, service levels maintained, and any faults are resolved through incident and problem management.
- During the Continual Process Improvement stage, the IT organisation collects and uses feedback from users, stakeholders, and customers to enhance and improve services.

A detailed overview of the Inputs, Outputs, and Links of the ITIL Service Lifecycle Stages is depicted in Figure 9.

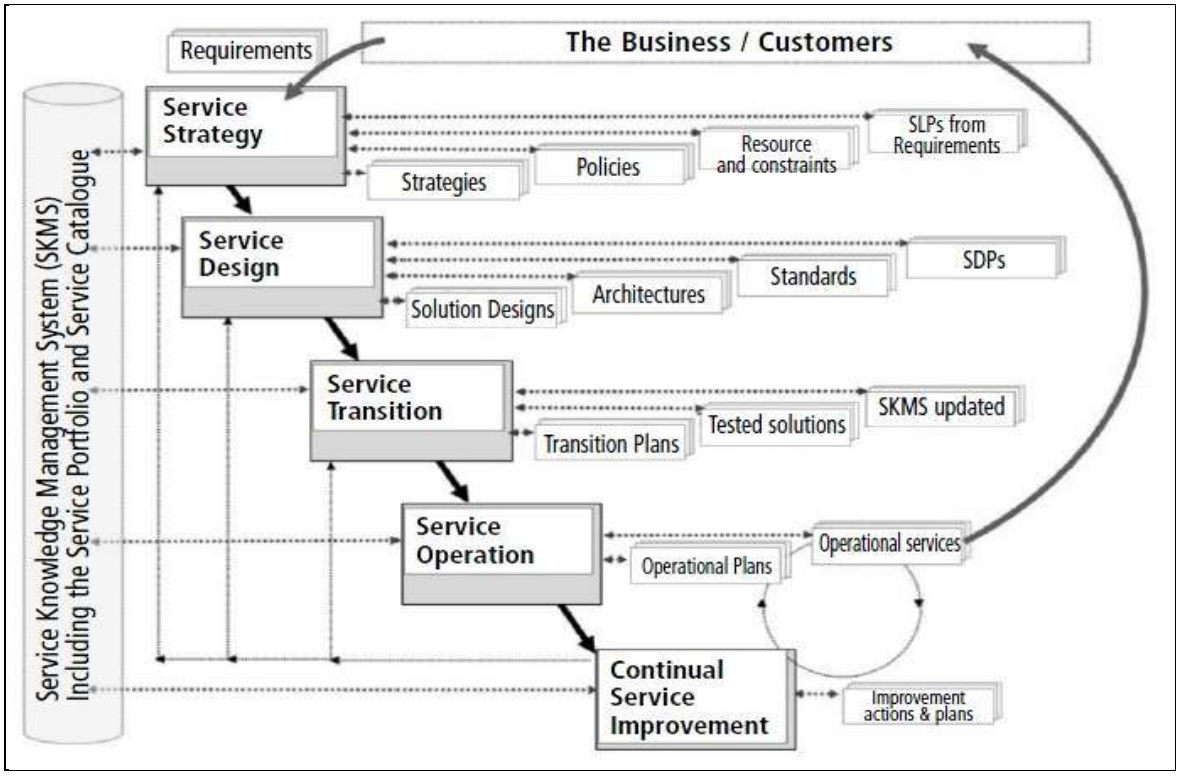

Figure 9: Inputs, Outputs of the ITIL Service Lifecycle

Source: Cartlidge et al, 2007

The lifecycle is initiated by a change in business requirements. These requirements are identified and agreed upon during the Service Strategy stage within a service level package (SLP) and a defined set of business outcomes.

This passes to the service design stage where a service solution together with a service design package (SDP) is produced. This will contain everything required to take it through the remaining stages of the lifecycle.

The SDP passes to the Service Transformation stage where the service is evaluated, tested, and validated. The service knowledge management system (SKMS) is updated and the service is transitioned into a live environment where it enters the Service Operations stage.

Wherever possible, Continual Service Improvement identifies opportunities for improving weaknesses or failures anywhere within the Lifecycle stages (Cartlidge et al, 2007).

2.4 Impact of Cloud Computing on IT Governance

There has been a major impact on IT budgets as a result of the economic downturn and organisations are now looking for solutions which offer better value at less cost. As a result, organisations are looking at new business models and new ways to offer services. The cloud seeks to replace the Capital Expenditure (CapEX) component of the current IT infrastructure with a “pay as you go” or Operational Expenditure (OpEX) model (KPMG, 2011). There are a number of CSP’s who offer cost savings, speed to market, less overheads, and global coverage (Lacy, 2012)**.** This is very attractive for businesses that have new ideas and no longer require large capital outlays to provide a service or the human capital to operate it. They also need not worry about over provisioning for a service whose popularity does not meet their expectations or under provision for a service which becomes very popular, thus missing potential customers and revenue (Armbrust et al, 2010).

One important aspect of IT governance is having in place the correct team structure and the right people involved in decision making. IT Governance, like most other governance activities, intensively engages both board and executive management in a cooperative manner.

While IT governance is the responsibility of the Board of Directors and Executive Management, the adoption of cloud services should be applied throughout the entire enterprise and especially between the IT function and the business units to ensure business requirements are met (IT Governance Institute, 2003). At Board level, short time to market and flexibility of cloud solutions provide Chief Executive Officer’s (CEO) with opportunities to support new business models or enhance existing services quickly. Tactically, the Chief

Financial Officer (CFO) and Chief Information Officer (CIO) are expected to play complementary roles where the CFO oversees financial evaluation while the CIO would analyse Total Cost of Ownership (TCO) and Return on Investment (ROI).

At an operational level, the IT teams and vendors play a key role in the implementation, migration, and deployment of cloud services. This would require ongoing monitoring and support for the service. Service Level Agreements (SLA) and Key Performance Indicators (KPI) would have to be constantly monitored to ensure the correct level of service is being provided to support the business. Cloud advisors would support each level at all times. They could also assist the organization in creating new service models, potentially triggering a radical change in the sector within which the organisation operates (KPMG, 2011).

The roles and responsibilities for delivery of cloud solutions are shown in Figure 10.

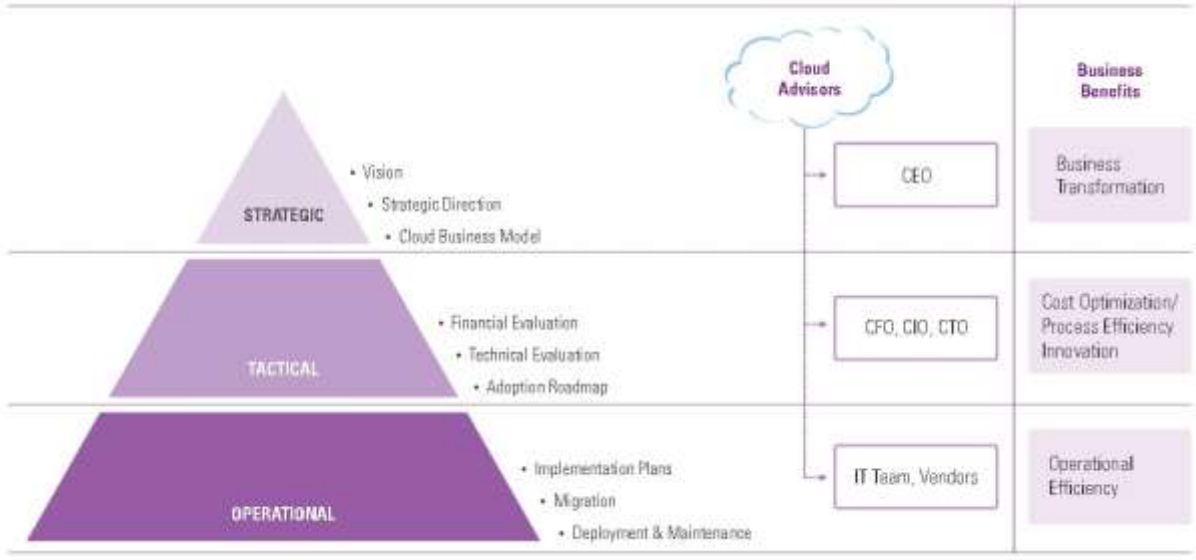

Figure 10: Roles and Responsibilities for Delivery of Cloud Solutions

Source: KPMG, 2011

2.4.1 Benefits of Cloud Computing

When considering cloud services, there are a number of benefits associated with this service. One such benefit is economies of scale. This can be everything from security where the same amount of investment in security buys better protection (Catteddu & Hogben, 2009), to physical data centers, where a private data center may not benefit from economies of scale that make public clouds financially attractive (Armbrust et al, 2010). This enables rapid, elastic, and smart scaling of resources which is so important for cloud services. The ability of the cloud provider to dynamically reallocate resources like authentication, encryption, resilience, and scaling out has its advantages (Catteddu & Hogden, (2009), Bisong & Rahman (2011), Romero & Stroud (2011)). Cloud computing is particularly

beneficial for small to medium businesses where effective and affordable information-based products are available without the expense of in-house resources and technical equipment. Additionally, there is the benefit of fewer maintenance costs on this equipment (Aymerich, Fenu, & Surcis, 2008). Cloud computing enables scaling on demand without the cost associated with building or provisioning a data center (Armbrust et al, 2009). As a result, this not only allows agile addressing of new markets and offerings to potential customers, but can also build tighter integration between business partners and end customers (Heier, Borgman, & Bahli, 2012).

2.4.2 Challenges of Cloud Computing

Conversely, there are a number of challenges and potential risks when adopting cloud services. Two areas of concern for organisations are Loss of Governance and Lock in (Catteddu & Hogden, (2009), ISACA, (2012), Heier, Borgman, & Bahli, (2012)). In respect to Loss of Governance, the organisation necessarily cedes control to the Cloud Provider potentially leaving gaps in security defences. With both Technology and Data lock-in, it is potentially difficulty for customers to migrate from one provider to another, or migrate data and services back to an in-house IT environment. The area of data security is another concern for organisations. This includes data protection, insecure or incomplete data deletion, and compliance risks in relation to the use of data. (Heier, Borgman, & Bahli, (2012), KPMG (2011), Cloud Security Alliance, (2009), Catteddu & Hogden, (2009), Chen, Paxon, & Katz, (2010)). Organisations need to ensure that effective data handling measures are in place. These include lawful handling of data, adequate and timely deletion of data when requested, and ensuring that correct roles and controls are in place for different users who have access to the organisations' data (ISACA, 2012). Finally organisations need to be confident that there are no compliance risks and that the cloud provider has achieved certification and will allow auditing by the cloud customer. They must also ensure that the compliance frameworks of both the organization and the cloud provider are aligned to meet their regulatory requirements (Catteddu & Hogben, 2009).

Organizations that have IT service management frameworks in place such as ITIL may worry about the impact that adopting cloud services will have on their existing framework. Steinberg & Clarke (2010) suggest that Core IT management disciplines for ITIL would not change and they would just move from the IT organization to the cloud service provider.

Service Strategy defines an IT organisation's high level approach to providing services. When implementing a cloud service, these services are provided by the cloud vendor and will have to be bundled and integrated with the IT services already in place. Strategic

decisions will be needed to align the cloud service with the right points in the existing IT Governance framework.

From a Service Design perspective, Cloud Service Providers will bundle service packages where business requirements and technical requirements feed into Service Catalogue Management (SCM), Service Level Management (SLM), and Capacity Management. These ITIL services need to be effectively coordinated to build a stable cloud solution that will benefit the business in the long term. Supplier Management is also critical to strengthen relationships between the business and Cloud Service Providers.

Traditionally, an IT organization would have readied a new or changed service for transition into operation. Since a vendor cloud is a shared responsibility environment, having an inclusive, structured Transition Planning and Support process and a responsible Project Planner is a critical success factor. Organizations should consider the appropriate notice that cloud vendors should give to the enterprise before implementing changes and releases and ensure that this is spelled out in service contracts. Once a service has been transitioned into operation, a traditional IT organization must ensure that expected value is delivered to the business and service disruptions are coordinated across suppliers. This is similar for the cloud vendor as the same value has to be delivered as from a normal IT organization.

During the Continual Process Improvement stage, the IT organisation collects feedback from users, stakeholders, and customers. This does not change for a cloud service. The cloud vendor should work with the business to provide a means to stay ahead of competition in the sector.

The shift in IT disciplines from the IT organization to the cloud vendor can be found in Figure 11.

Figure 11: Shift in IT Disciplines

Source: Steinberg & Clarke, 2010

Adopting a Cloud Service Strategy is a serious undertaking for any organization and there is a real need to understand potential problems that may impact the business by following this strategy. Gartner (2010), Kaliski & Pauley (2010), Wyld (2010), Chen (2009), suggest that a Risk Assessment or Cloud Readiness Assessment should be carried out by any organization wanting to embrace a Cloud Service Strategy. This will help IT managers not only understand the service they are adopting but also understand if their organization has the capability and wherewithal to successfully manage the service and provide value back to the business.

Chapter 3: Findings

3.0 Introduction

In this chapter the main findings of the empirical research are discussed, including the outcome of a number of interviews, each objective, and also the result of the Cloud Readiness Assessment which was tested on a CSP.

3.1 Findings

Objective: *What considerations are taken into account by companies when they move their data or client's data to a Cloud Service Provider?*

In line with Lacy (2012), KPMG (2011) and Armbrust et al (2009, 2010) this research found that there are a number of reasons why companies look at cloud services as they provide an attractive alternative to tradition IT solutions. Research shows that key benefits of a cloud service are agility, scalability and elasticity. Agility allows access to new markets and potential customers, and builds tighter integration between the business partner and end customers. Observations from the research reinforce this. Selecting a cloud service offering enabled Company A to develop a new web-based solution which presented new opportunities and new markets and thus generated new interest from customers. The solution has been designed in such a way as to allow scalability and flexibility to meet the expected increase in business.

Furthermore, in line with (Catteddu & Hogden, (2009), Bisong & Rahman (2011), Romero & Stroud (2011) this research found that dynamic scalability and resilience to meet business needs are very important. To address the increase in demand, the research showed that the company needed to be comfortable with capacity management. The research suggested that the core IT management disciplines would not change, just move from the IT organization to the cloud vendor. Here we can see the importance of the cloud service provider providing capacity management which is essential for on demand, disruption-free service delivery. From the master service agreements and the research, it can be seen that it was deemed so important that the cloud vendor would be penalized commercially if issues arose around availability, scalability, or performance. When drawing up the service level agreements with the CSP, the company had long discussions with their Legal team and the company data protection officer to ensure that the right SLAs were in place. These agreements have to be in place due to the sensitive nature of the data and particularly if data moves from one jurisdiction to another. One observation made from the CSP's Master Service Agreements is that if legal action was to take place for any reason, the cloud service

provider would only deal with a certain state in the U.S. This could potentially impact any case that may be taken against the cloud service provider.

The research shows that cost was a key factor for moving to a cloud-based service, Armbrust et al (2010), Lacy (2012), Aymerich, Fenu & Surcis (2008), but this research found that this was not explicitly a factor for implementing this cloud solution. Observations from the research of Company A concluded that business partners are driving the selection process. As a service provider, Company A's business partners are looking at the customer or end user needs and identifying solutions that will meet those needs. The patterns of business activity are driving the demand for these services and, as a result, cloud offerings are being aligned to meet the business needs.

In line with Catteddu & Hogden, (2009), ISACA, (2012), Heier, Borgman, & Bahli, (2012) this research found that there are a number of areas of concern for businesses moving data to the cloud, including data governance, security, data handling, and potential data lock-in. As part of their due diligence, Company A employed an independent company to perform security penetration testing and risk assessments of the CSP. The audit process was very important for Company A since an audit trail has to be in place due to compliance and regulatory requirements. One observation from the research suggested that if an auditing company was used, they must be accredited and produce a report that conforms to a reporting framework, for example, Service Organization Control (SOC 2). It was also suggested that ISO27001 certification is very important but it was highlighted that you need to understand what it covers and what is in scope. A number of controls can be left out, so you need to understand what they are and how they affect the data centers. The situation may arise where only two out of three data centers are certified, which would result in it being meaningless for what you want. It was also suggested to use a security questionnaire which will be signed off by their security officer. This would cover all aspects including infrastructure, application portal, and security programme.

In line with Heier, Borgman, & Bahli, (2012), KPMG (2011), Cloud Security Alliance, (2009), Catteddu & Hogden, (2009), Chen, Paxon, & Katz, (2010) another observation was the importance of data segregation and an understanding of what safeguards are in place. The research suggested that there have to be sufficient safeguards in place for data segregation and this includes data encryption when at rest and in flight. This ties into confidentiality, integrity, and availability and it was suggested that each company might have a different view on this. Confidentiality might be important to a lot of companies but integrity of data is very important for Company A.

Furthermore in line with Heier, Borgman, & Bahli, (2012), KPMG (2011), Cloud Security Alliance, (2009), Catteddu & Hogden, (2009), Chen, Paxon, & Katz, (2010) the research found that, in relation to data governance and data handling, the entire data lifecycle process has to be handled and managed properly. This includes everything from security of data being shipped offsite, purging of old or expired data, to data management if the contract is terminated or the company goes out of business. The use of the questionnaire, requesting audit reports, penetration test results, and ISO certification provides the company with a certain amount of comfort. Should Company A be audited by their business partners, it has all the information in place and can provide answers to why they selected a certain CSP. In turn, Company A can give the CSP a certain risk rating.

Objective: *How do you match your IT Governance framework to the IT Governance framework of a cloud provider?*

In line with KPMG (2011) and IT Governance Institute (2003) which suggests that the adoption of cloud services should be addressed at all levels in an organisation, this research found that this is not the case with Company A. Whilst a number of areas like the Company Board, Business units, and IT Architecture were involved in the solution design and decision, one observation is that it was made absent traditional IT teams like Operations and Service Desk. This has been identified as a gap and a risk, because as the research suggests, operational level IT teams and vendors should play a key role in the delivery of cloud services. However, in line with KPMG (2011), this research found that Company A has engaged with cloud advisors to support their solution.

Another observation from the research suggested that the transition of the service into production provided a significant number of challenges for company A. In line with Steinberg & Clarke (2010), this research found that traditionally the IT organization would have performed this activity, but as this core IT management discipline was moving to the cloud a greater amount of collaboration with the CSP was required. Due to the cloud aspect, the research found that it required a lot of process redesign and refinement. This also resulted in a number of discussions with the business to allow them to understand the concept and benefits to the business. The research found that, like all changes, it was important to get user buy-in as early as possible. Key to this was the involvement of a large team of change managers. Their primary responsibilities were developing the communications, the change rationale, and the benefits message to the users so they would embrace the new technology. Engagement with end users throughout the project and change management were seen as bringing an extra dimension to the project particularly at senior level, and thus improved the overall communication around the change.

In line with Kim (2003), Wessels & Van Loggerberg (2006), Van Grembergen et al (2004b), Long (2008) and Cartlidge et al (2007), this research found that Company A had implemented a number of aspects of the ITIL Governance framework, but also revealed a number of serious gaps which could potentially pose a risk to the business. One important aspect is the use of a Service Catalogue. Research suggests that both the business and technical requirements feed into this, but Company A currently has no service catalogue in place. The research identified this as a huge gap in Company A's IT governance framework and service definition. The second gap identified was the lack of a content management database (CMDB) which is a repository of information related to all components of the information system that provides a view of what you have in the IT environment and is an important aspect of any service transition from test into production. However, Company A does maintain a supplier management database which is a critical process to strengthen relationships between the company and its CSP. Companies on this list must sign up to a confidentiality agreement, and also adhere to Company A's ethics and compliance guidelines. This is reviewed annually by Company A's vendor management team.

Another important aspect of the ITIL framework is the normal day-to-day change process. In Company A, changes are coming in through the business and not through IT as there is no formal process in place to manage cloud service changes. This was seen as a significant issue which needed to be addressed. As mentioned previously, agility and flexibility are seen as strengths but also seen as a weakness for Company A. The interviewee highlighted that if a CSP produced a release plan, there was no choice or any option about having it implemented. The concern was whether these changes were backward compatible or would require re-training users on a new version of software. Currently, in Company A these changes are not going through change control and are a potential risk to the business. From the master service agreements, the CSP does outline a maintenance plan, which is very important, but a large cloud service provider could have hundreds of changes so it would be unrealistic for every change to go through Company A's change process. Large changes, however, could be highlighted and go through the company's change control process. This is why SLAs and master service plans are so important, as they will highlight the change process and how rigorously changes are tested before being deployed. From an ITIL perspective, when the core IT management discipline of service operations is moved from the IT organisation to the cloud vendor, it is important that the service and changes to the service are delivered without disruption.

Incident management and problem management form another important part of the ITIL Governance Framework. Traditionally, Company A's IT organisation would have worked

directly with the service desk. In Company A, the cloud service falls outside the normal IT function, so another team works directly with the CSP. One observation from the research was the concern over incident management. Currently, there is no process in place to log incidents through the Service Desk and this is seen as a risk to the business and a gap in the ITIL Framework which needs to be reviewed. Whilst the priority levels for incidents have been laid out by the CSP in the master service agreement, these have not been aligned to that of Incident management.

The final aspect of the ITIL governance framework is Continual Service Improvement. It was observed from the research that the commercial aspect of the service is very important and there was a motivation there for the CSP to supply a good service, and as a result get more traffic to use the service. The CSP is actively promoting the service with the goal of continuously creating benefit for the business.

A number of Key Performance Indicators (KPI) are embedded in the service. This is due to the fact that the key business drivers of compliance and inspection readiness can be satisfied and measured for any audits that take place. It was noted that Company A is in a strong position and enjoy greater benefits because they are a larger customer of the CSP. However, it was noted that this may change as new customers come on board.

Objective: *What type of cloud readiness assessment if any are taken by companies?*

In line with Gartner (2010), Chen (2009), Kaliski & Pauley (2010), Wyld (2010), this research found that Company A did perform risk and due diligence assessments prior to the deployment of a cloud service but no Cloud Readiness Assessment was performed. One of the main observations from this is that the due diligence performed by the company was outward facing and focused on the CSP. The research indicated that this is certainly a requirement but the process did not look inwards at the company itself. There was no real recognition of the IT Governance framework (ITIL) which was in place in the company, or how the new cloud service would integrate into this framework. As part of the due diligence, testing different aspects were examined, such as data security, access to data, and network security but the project did not set out with the intention of integrating the cloud service into the ITIL Framework. As a result, gaps in the process such as incident, problem and change management, service catalogue, and CMDB have been identified.

3.1.1 Cloud Readiness Assessment

Following the interviews which were conducted with Company A, the Cloud Readiness Assessment was created in order to prepare a business for a move to a CSP and assess the

suitability of the service. It is structured in such a way as to provide an initial assessment of the CSP while also focusing on the organisation's ITIL Governance framework. In doing so, it allows for an outward view of the CSP but also allows an inward assessment of the organisation IT Governance Framework. The assessment was tested on a CSP and provided very good insight to the service they were providing while also covering all aspects and gaps identified in the ITIL Governance framework. Among its key findings, this assessment:

- Took one hour and gave a very good overview of the service being provided.
- Allowed quick identification of business concerns such as data lock-in, data governance, and security.
- Quickly identified how flexible the solution would be in terms of performance and scalability
- Identified the pricing structure and how flexible this is. This enabled the business to understand the cost associated with the service.
- Provided insight to how redundant the solution was: i.e. disaster recovery plan and data centre operations. It also covers the SLAs with which the service provider will comply.
- Covers a number of areas in relation to security such as encryption, multi- tenancy, and data lifecycle management. It also looks at auditing, a key business driver.
- Looked at how the solution would be transitioned into production and what support is in place once in production.
- Covers solution release, deployment, and ongoing maintenance schedule.
- Looks at Key Performance Indicators and Continual Service Improvement which are required in order to meet the business needs.

The Cloud Readiness Assessment used on the Cloud Service Provider is shown below.

- ☐ External – Questions focused on Cloud Service Provider
- ☐ Internal – Questions focused on the Company and their IT Governance Framework (ITIL)

Business / Customer

- ☐ What Cloud Services do you provide?
- ☐ How flexible is your Cloud offering?
- ☐ How will I access my data and applications in the Cloud?
- ☐ Can you provide us with details on successful similar deployments of your service?
- ☐ Can we talk to your customers?
- ☐ What is the process for setting up the solution?

Service Strategy

Demand Management

- ☐ External – How does your Cloud offering scale to meet our requirements?
- ☐ Internal – What are the business requirements, patterns of activity, and has growth been factored in? (Identify Product Manager/Service Owner and Business Relationship Manager)

Financial Management

- ☐ External – What is your Pricing Structure and is there Price Protection?
- ☐ Internal – Identify revenue cost, cost to deliver service, budgets, and is the financial decision making team in place? (CFO, CIO, Finance Dept.)
- ☐ External – Is there flexibility in your Master Level Agreements or Terms of Service?
- ☐ Internal – Are Financial, Legal, Contracts, and Vendor Management decision making team in place?

- ☐ External – Is there financial compensation for not meeting SLA's?
- ☐ Internal – Are Financial, Legal, Contracts, and Vendor Management decision making team in place?
- ☐ External – How can we test this service before we make a decision?
- ☐ Internal – Are the correct resources available and a Cross Functional Team in place to test the service?

Service Portfolio management

- ☐ External – What is your Product Road Map and how will your service be developed in the future?
- ☐ Internal – Are Service owner/Product manager, Business Relationship Manager, and CIO in place and available to review the solution and govern the investment?

Service Design

Information Security Management

- ☐ External – Who can see my data?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to review or create Information Security Policy?
- ☐ External – Can you outline if you offer dedicated resources, multi tenancy or mixture of both?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to review or create Information Security Policy?
- ☐ External – How do you handle co-location of data in relation to isolated and safeguarded from other clients?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to carry out Business Impact Analysis (BIA) and Risk Analysis?
- ☐ External – What is your data encryption policy and how do you encrypt data?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to create review security controls?

- ☐ External – What certificates for data encryption do you have?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved?
- ☐ External – How do you manage encryption keys?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to create Information Security Management System (ISMS)?
- ☐ External – Tell me about your datacentre, specifically its Location, Security policy, Access Policy?
- ☐ Internal – Are IT Security Team and Facilities involved to define level of security and control?
- ☐ External – How can you continue to provide protection as my workload evolves?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to document processes and controls?
- ☐ External – Can we review your ISO and SOC certification for the datacentre where our data will reside and also for the datacentre where the services would potentially failover to?
- ☐ Internal – Are IT Security Team and Data Protection Officer involved to review and understand if the documentation is correct and suits the needs of the company?

Availability Management

- ☐ External – What data durability do you have, i.e. five nines or ten nines?
- ☐ Internal – Are IT Operations and Business Continuity Teams involved to review Availability Management Information System?

IT Service Continuity Management

- ☐ External – What is your Downtime History?
- ☐ Internal – Do Business and Business Continuity Teams need to review Availability Management Information System.?
- ☐ External – Do you have a comprehensive Disaster Recovery Plan?
- ☐ Internal – Are Business Continuity and Disaster Recovery Teams involved to review Availability, Reliability, Maintainability, Serviceability, and component Availability?

- ☐ External – Do you have a comprehensive Business Continuity plan?
- ☐ Internal – Are Business Continuity and Disaster Recovery Teams involved to review Availability, Reliability, Maintainability, Serviceability, and component Availability?
- ☐ External – What happens if you lose data?
- ☐ Internal – Is there an organisation-wide process in place to deal with business or client data loss?

Capacity Management

- ☐ External – Do you work with customers on Capacity Management to meet business needs?
- ☐ Internal – Is there a Capacity Management plan is place to manage this process and provide advice and guidance to IT and the business?

Service Level Management

- ☐ External – What are your Service Level Agreements and can we review your history of service level management?
- ☐ Internal – Is the key interface of Service Level Management in place to review Service Level Agreements and contracts?
- ☐ External – Do you have Service Level Agreements and Operational Level Agreements with your own service providers? Can we review these to ensure they align with ours?
- ☐ Internal – Is the key interface of Service Level Management in place to review Service Level Agreements and contracts?
- ☐ External – What is your customer support service offering?
- ☐ Internal – Are Service Delivery Management involved so as to agree support levels and procedures?
- ☐ External – How easy is it to migrate to another cloud service provider?
- ☐ Internal – Is there cross-team involvement to understand what the exit strategy will be?
- ☐ External – How much control do I retain over my data?

- Internal – Is there cross-team involvement to understand the levels of data control required and also confirm what the exit strategy will be?

Supplier Management

- External – Which parts of your cloud service and infrastructure are outsourced?
- Internal – Is there a Vendor Relationship manager in place to maintain supplier and contractor database and review annually?
- Internal – Ensure Service Catalogue Management is in place and ensures information is accurate and current.

Service Transition

Transition Planning and Support

- External – How are service transitioned from test into production?
- Internal – Ensure all Teams are in place for transition and that the Configuration Management Database (CMDB) is in place.

Change Management

- External – How do you schedule maintenance and manage upgrades/changes?
- Internal – Change = Risk so confirm that Change Management process is in place for all levels of change including release and deployment.
- External – What visibility is there into this process?
- Internal – Change = Risk so confirm that Change Management process is in place for all levels of change including release and deployment.

Knowledge Management

- External – Do you have a location where information about your service is located?
- Internal – Is there a knowledge management database in place for the new solution?

Service Operation

Incident and Problem Management

- ☐ External – Do you provide Operational Transparency particularly around Monitoring, Incident, and Problem management?

- ☐ Internal – Service Operations is where Value is seen. Does the organisation have correct processes in place for Incident, Problem, and Event management?

- ☐ External – How is activity on my cloud infrastructure monitored and documented? Can we review who has accessed our infrastructure on behalf of the cloud provider?

- ☐ Internal – How will the organisation monitor and manage the service and what processes are in place?

- ☐ External – Do you have a public site listing issues and outages?

- ☐ Internal – How will the organisation monitor and manage the service and what processes are in place to communicate any issues which occur?

- ☐ External – How do you manage incidents and problems with your customers?

- ☐ Internal – Does the organisation have correct processes in place for Incident, Problem, and Event management and what is the Service Desk involvement in the process?

- ☐ External – Is this aligned to customer's incident/problem management framework?

- ☐ Internal – Does the organisation have correct processes in place for Incident, Problem, and Event management and what is the Service Desk involvement in the process?

Request fulfilment

- ☐ External – Do you have self-help options for request fulfilment?

- ☐ Internal – What process is in place to request a change or manage a change?

Access Management

- ☐ External – How do you ensure client endpoint protection?

- ☐ Internal – Has the organisation put measures in place for requesting, verifying, and monitoring access to the service?

- ☐ External – Can I leverage existing credentials and passwords and disable access immediately?

- ☐ Internal – Has the organisation put measures in place for requesting, verifying, and monitoring access to the service? Is it done through the Service Desk?

- ☐ External – What happens if an employee leaves, joins, or changes roles in the Cloud Service Provider? Can they access our data?

- ☐ Internal – Has the organisation a matching process for employees? Is it done through the Service Desk?

- ☐ External – How can I be assured my data is protected?

- ☐ Internal – Does the organisation have an Audit team available or a third party to monitor the service?

- ☐ External – Do you allow Audits of your environment?

- ☐ Internal – Does the organisation have an Audit team available or a third party to audit the service?

Continuous Service Improvement

- ☐ External – What KPI's are used to ensure service across the cloud and how are they reported?

- ☐ Internal – Does the organisation understand what it wants from the KPI's?

- ☐ External – What measurements are taken to ensure service objectives are being met?

- ☐ Internal – Is there a continual service improvement model in the organisation?

- ☐ External – How do you work with customers to proactively improve services?

- ☐ Internal – How does the organisation manage feedback good or bad?

Chapter 4: Conclusion

4.0 Introduction

The focus of this research is to understand the impact of cloud computing on IT Governance and in particular, the ITIL Governance Framework. Company A currently uses Cloud Services and the premise of this research was to understand the impact cloud computing would have on their IT Governance Framework. This chapter reviews the objectives of the study and how well the objectives have been achieved. The Cloud Readiness Assessment will also be reviewed and finally we will look at how it will help in the alignment of Company A's IT Governance Framework and the Cloud Services that they are providing to the business.

4.1 Assessment of Results

This report set out to answer the following research question:

What is the impact of cloud computing on IT Governance (ITIL)?

This was met through three objectives which in turn led to the creation of a Cloud Readiness Assessment. The purpose of which was to enable the company to align the Cloud Service with their IT Governance Framework to ensure there were no gaps which could potentially pose a risk to the business.

In respect to the first objective—*What considerations are taken into account by companies when they move their data or client's data to a CSP?* —it can be concluded that Company A took a number of considerations into account when selecting a cloud service solution. Due to the patterns of business activity, the solution was designed in such a way as to allow scalability and flexibility to meet the expected increase in business. These included performance, demand, and capacity management. Operational level IT teams were not involved in the selection and this was identified as a risk to the business. Service level agreements were put in place to ensure service availability and continuity and financial penalties are in place if they are not met. Company A paid particular attention to the area of security and data management with the use or risk assessments and penetration testing.This is very important for auditing purposes due to compliance and regulatory requirements.

In respect to the second objective—*How do you match your IT Governance framework to the IT Governance framework of a CSP?*—it can be concluded that a number of gaps in relation to Company A's IT Governance Framework have been identified and as a result present a

number of potential risks to the business. These included such things as lack of proper incident, problem, and change management for the cloud service as well as lack of a service catalogue and CMDB, all of which need to be addressed.

In respect to the final objective—*What type of cloud readiness assessment if any are taken by companies?*—it can be concluded that whilst the company did not perform a Cloud Readiness Assessment, they did perform in-depth due diligence testing of the cloud solution. This testing was very important but it concentrated outward on the cloud service and not inward at the company to establish if the company's ITIL framework was ready to support this service.

The Cloud Readiness Assessment proved very successful and helped provide an overall view of the Cloud Solution. These results can be used by the company to remedy all gaps and issues which were identified in their IT Governance Framework.

4.2 Limitation of the Research

Whilst this study reached its aims through its objectives there are a number of limitations to this research. First of all the research only focused on one company. Further research on other companies would have given a better understanding on the impact of cloud computing on IT Governance. Researching other companies would have given a better perspective on the situation with cloud computing and its impact on IT Governance. Another limitation of this study is the number of interviews that were conducted. Three interviews were conducted in Company A which gave a good overview of the cloud service but another interview with senior management would have yielded further information on vision and direction of cloud services and IT governance in company A. Furthermore only one CSP was interviewed using the Cloud Readiness Assessment as part of the study. This research would have benefited from the inclusion of other CSP's who had a larger number of customers. This would have provided a view where a company is one of a number of thousand customers using the cloud service.

Chapter 5: Bibliography

Al Morsy, M., Grundy, J., & Muller, I. (2010). An Analysis of The Cloud Computing Security Problem. *APSEC 2010 Cloud Workshop* (pp. 1-6). Sydney: In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

Anthes, G. (2004). *Model Mania.* Global: Computerworld.

Armbrust et al. (2009). Above the Clouds: A Berkley view of Cloud Computing. *Electrical Engineering and Computer Sciences University of California at Berkeley*, 1 - 23.

Armbrust et al. (2010). A View of Cloud Computing. *Communications of the ACM*, 50-58.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Konwinski, A., & Lee, G. (2010). A View of Cloud Computing. *Communications of the ACM*, 50-58.

Aymerich, F., Fenu, G., & Surcis, S. (2008). *An Approach to a Cloud Computing Network.* IEEE.

Berger, I. (2009, January 24). *http://cloudcomputing.sys-con.com/node/612375?page=0,2*. Retrieved from http://cloudcomputing.sys-con.com: http://cloudcomputing.sys-con.com/node/612375?page=0,2

Bisong, A., & Rahman, S. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1,*, 30-45.

Britten, N. (1995). Qualitative interviews in medical research. *British Medical Journal*, 251-253.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. (2007). *itSMF - An Introductory Overview of ITIL® V3.* UK: The UK Chapter of the itSMF.

Catteddu, D., & Hogben, G. (2009). *Cloud Computing - Benefits, risks and recommendations for information security.* European Network and Information Security Agency.

Chen, D. (2009). Information Security and Risk Management. *Encyclopedia of Multimedia Technology and Networking*, 1-15.

Chen, Y., Paxon, V., & Katz, R. (2010). *What's New About Cloud Computing Security?* Berkley: Electrical Engineering and Computer Sciences University of California at Berkeley.

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

Creswell, J. (2003). *Research design: Qualitative, quantitative and mixed methods approaches (2nd ed.).* Thousand Oaks: SAGE Publications.

Dul, J., & Hak, T. (2008). *Case Study Methodology in Business Research.* Oxford: Elsevier LTD.

Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review, Vol. 14, No. 4*, 532-550.

Foster et al. (2008). Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environments Workshop (GCE '08)* (pp. 1-10). Austin: Institute of Electrical and Electronics Engineers (IEEE) .

Gartner. (2010). *Cloud Computing: The Next Generation of Outsourcing.* Stamford USA: Gartner.

Giordanelli, R., & Mastroianni, C. (2010). The Cloud Computing Paradigm:Characteristics, Opportunities and Research Issues. *Consiglio Nazionale delle Ricerche Istituto di Calcolo e Reti ad Alte Prestazioni*.

Heier, H., Borgman, H., & Bahli, B. (2012). Cloudrise: Opportunities and Challenges for IT Governance at the Dawn of Cloud Computing. *45th Hawaii International Conference on System Sciences* (pp. 4982-4991). Hawaii: IEEE Computer Society.

http://www.hci-itil.com. (2013, January 29). *Overview of the ITIL v3 Library*. Retrieved from http://www.hci-itil.com: http://www.hci-itil.com/ITIL_v3/references/ITIL_v3.html

ISACA. (2012). *Cloud Computing Market Maturity Study Results.* Ilinois: ISACA.

IT Governance Institute. (2003). *Board Briefing on IT Governance.* USA: IT Governance Institute.

Kaiserswerth et al. (2012). Cloud Computing. *Swiss Academy of Engineering Sciences*, 1-51.

Kaliski, B., & Wayne, P. (2010). *Toward Risk Assessment as a Service in Cloud Environments.* Boston MA: EMC Corporation.

Kephart, J., & Chess, D. (2003). The Vision of Autonomic Computing. *IEEE*, 41-50.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). *Research Challenges for Enterprise Cloud Computing.*

Kim, G. (2003). Sarbanes-Oxley, Fraud Prevention, and IMCA:A Framework for Effective Controls Assurance. *Computer Fraud & Security*, 12-16.

KPMG. (2011). *The Cloud - Changing the Business Ecosystem.* India: KPMG.

Kvale, S. (1996). *Interviews: An Introduction to Qualitative Research Interviewing.* California: Sage Publications .

Kvale, S., & Brinkman, S. (2009). *Interviews : Learning the craft of Qualitative Research Interviewing.* California: SAGE Publications LTD.

Lacy, S. (2012, 03 13). *www.Best-Management-Practice.com.* Retrieved from www.Best-Management-Practice.com: www.best-management-practice.tv/seminars/ITIL_and_The_Cloud.pdf

Livetime. (2013, January 29). *ITIL v3 Service Management Lifecycle – Part 1*. Retrieved from www.Livetime.com: http://blogs.livetime.com/itil-3-service-management-lifecycle-part-1/

Lohr, S. (2007, October 8). *www.nytimes.com*. Retrieved from www.nytimes.com: http://www.nytimes.com/2007/10/08/technology/08cloud.html?_r=0

Long, J. (2008). *ITIL Version 3 at a Glance.* North Carolina: Springer.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology*, 1-3.

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly (21:2)*, 241-242.

Patel, N. (2002). Global Ebusiness IT Governance: Radical Re-Directions. *IEEE Computer Society*.

Pritzker, J. (2009, January 24). *http://cloudcomputing.sys-con.com/node/612375?page=0,1*. Retrieved from http://cloudcomputing.sys-con.com: http://cloudcomputing.sys-con.com/node/612375?page=0,1

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. *Proceedings of the 37th Hawaii International Conference on System Sciences .* Hawaii.

Romero, S., & Stroud, R. (2011). *IT Governance and the emergence of cloud computing:Using project and portfolio management to make effective cloud decisions .* CA Technology.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students, 5th ed.* Harlow: Pearson Education.

Steinberg, R., & Clarke, N. (2010). Cloud computing: Is ITIL still relevant? *HP Software Universe 2010* (pp. 1-42). Deloitte.

The National Computer Center. (2005). *IT Governance - Developing a Successful Governance Strategy.* Manchester: The National Computing Centre.

van der Aalst, W. (2010). Configurable services in the cloud:Supporting Variability While Enabling Cross-Organizational Process Mining. *Eindhoven University of Technology, The Netherlands*.

Van Grembergen et al. (2004b). Structures, Processes and Relational Mechanisms for IT Governance. *Idea Group Publishing*, 1-36.

Van Grembergen, W. (2002). Introduction to the minitrack IT governance and its mechanisms. *Proceedings of the 35th Hawaii International Conference on System Sciences.* Hawaii: IEEE.

Van Grembergen, W., & De Haes, S. (2004a). IT Governance and Its Mechanisims. *Information Systems Control Journal*, Volume 1.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004b). Structures, Processes and Relational Mechanisms for IT Governance. *Idea Group Publishing*, 1-36.

Van Grembergen,W & De Haes, S. (2004a). IT Governance and Its Mechanisims. *Information Systems Control Journal*, Volume 1.

Vaquero et al. (2009). A Break in the Clouds: Towards a Cloud Definition. *Computer Communication Review*, 50-55.

Wessels, E., & van Loggerenberg, J. (2006). IT Governance: Theory and Practice. *Proceedings of the Conference on Information Technology in Tertiary Education.* Pretoria.

Williams, C. (2007). Research Methods. *Journal of Business & Economic Research Vol 5 no 3*, 65-71.

Wladawsky Berger, I. (2009, January 24). *http://cloudcomputing.sys-con.com/node/612375?page=0,2*. Retrieved from http://cloudcomputing.sys-con.com: http://cloudcomputing.sys-con.com/node/612375?page=0,2

Wyld, D. (2010). The Cloudy Future of Government IT:Cloud Computing and the Public Sector around teh World. *International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1*, 1-20.

Yin, R. (2003). *Case Study Research: Design and methods, 3rd edition.* London: SAGE.