UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

CLOUD COMPUTING GOVERNANCE READINESS ASSESSMENT: CASE STUDY OF A LOCAL AIRLINE COMPANY

By

STEPHEN OUMA OWUONDA

(P54/73246/2014)

Supervisor

DR. DANIEL O. ORWA

This project report is submitted in partial fulfillment of the requirement for the award of Masters of Science in Information Technology Management of the University of Nairobi.

April, 2016

DECLARATION

This is to certify that this research project is a product of my original research investigation and has not been presented for a degree award in any other university or institution of higher learning. Information from other sources has been acknowledged.

STEPHEN OUMA OWUONDA

Reg No: P54/73246/2014 Date.....

Sign.....

This research project has been submitted as part of fulfillment of requirements for the Master of Science in Information Technology Management with my approval as the Supervisor.

Dr. DAN ORWA Date.....

Sign.....

ABSTRACT

Cloud computing has emerged as an important platform to organizations seeking innovative ways to save money and increase the trust and value of their information systems. It has shifted the traditional IT paradigm by extending Information Technology's existing capabilities by offering high scalability capabilities, reduced time to market, transformation of CAPEX to OPEX thus offering cost advantages as well as efficient use of computing resources due to pay-per-use nature of cloud services.

To reap the many benefits cloud computing offers, an organization needs to have a clear cloud governance framework, which must be continually improved to address the emerging cloud computing challenges. Many cloud consumers have extended their IT governance frameworks to their cloud services; however, these frameworks don't adequately address governance challenges in cloud environments. Additionally, most consumers don't have quantitative mechanisms to measure their cloud computing governance maturity, and therefore may not identify the opportunities to improve their cloud governance frameworks to attain a higher maturity level.

This research developed a conceptual model, which was used to analyze the cloud computing readiness of a local airline company. Path analysis was used to evaluate the correlation between the various model components and effective cloud governance, and to what extent these components contribute to effective cloud governance.

From the path analysis results, existence of expectation management, capacity management, change management, risk management, security management and exit strategy were established to be necessary for effective cloud governance. The *beta* correlation co-efficient values were summed and compared with the class limits of a model developed from the cloud computing capability maturity model to assess the cloud governance readiness of the organization. The total of *beta* correlation co-efficient values from path analysis was 3.048, which falls within the limits of initial level of cloud governance maturity level.

Finally, the research recommended multi-factor authentication, definition clear encryption key management responsibility, clear backup and recovery procedures, formulation of cloud exit policy as well as proper resource management; both human resources as well as computing resources as the necessary drivers towards achieving a higher cloud governance maturity level.

ACKNOWLEDGEMENT

I thank the almighty God for his care during the research period.

Special thanks to my supervisor Dr. Daniel Orwa for his guidance and valuable input in conducting this research. I'd also like to salute the entire examining panel consisting of Dr. Daniel Orwa, Professor P. W. Wagacha, Mr. Christopher Moturi and Mr. Samuel Ruhiu for their contributions and guidance throughout the research period.

Many thanks to my friend Erick Wao whose contribution was immense especially in path analysis.

Lastly, I thank all the respondents who took their time to fill and submit the online questionnaires and those who participated in focus group discussion. Without the valuable information you provided, this research wouldn't be a success. May God bless you abundantly.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACL-Access Control Lists
BPaaS-Business Process as-a-Service
CAPEX-Capital Expenditure
CC-CCM-Cloud Computing Capability Maturity Model
CCM- Capability Maturity Model
COBIT® - Control Objectives for Information and related Technologies
CRM-Customer Relationship Management
CSA-Cloud Security Alliance
CSP- Cloud Service Provider
EAS-Advanced Encryption Standard
FGD- Focus Group Discussion
I.S. – Information Systems Department or Function
IaaS-Infrastructure-as-a-Service
IAM-Identity and Access Management
IDC-International Data Corporation
IM-Identity Management
IP-Internet Protocol
ISAE - International Standards Assurance Engagements
IT – Information Technology
NIST- National Institute of Standards and Technology
OP Manager-Operation Manager
OPEX-Operating Expenditure
PaaS-Platform-as-a-Service
SaaS- Software-as-a-Service
SAS - Statement on Auditing Standards
SCAP- Security Content Authentication Protocol
SEI – Software Engineering Institute
SLA- Service Level Agreement
SOA- Service Oriented Architecture
SSAE – Statement of Standards for Attestation Engagements
SSL-Secure Socket Layer
VM-Virtual Machine
VPN- Virtual Private Network

CHAPTER 1: INTRODUCTION

1.1 Background to the Research

Cloud computing has emerged as an important platform to organizations seeking to increase trust and value of their information systems, as well as those seeking innovative ways to save money. Organizations across business and public sector spectrum are either moving to cloud or thinking about cloud (Trivedi, 2013). It offers organizations benefits such as optimized server utilization, cost savings to clients by transitioning capital expenses (CAPEX) to operating expenses (OPEX), dynamic scalability of IT power for clients, shortened lifecycle for development of new applications or deployments, and shortened time requirements for new business implementations. The NIST 800-145 defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand and network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". There are various success factors for cloud success. Agile Path, a renowned IT research company identifies three pillars of cloud computing as **cloud-centric leadership**, **cloud governance** and **cloud management**. As Agile path observes, every new piece of technology usually creates a vacuum in the form of key IT disciplines that will help with the adoption, insertion and value creation from that new technology. Generally, IT acquisition processes tend to be strained with new technologies. Typically, industry standards tend to lag behind for early adopters of these new technologies. Proven methodologies and guidance are always missing for such technologies.

Oracle (2009) noted that more than 75% of the annual IT budget is spent on the cost for operating and managing the applications. However, Tan et al. (2012) states that it's vague to identify whether or not those applications are really deriving business values to the organization. They further add that this leads to the IT application redundancy issue where similar IT applications produce the similar functionalities in business. Tan et al. therefore suggest that application rationalization is one of the ways to disentangle this issue. They state that adopting cloud services (SaaS) is a potential option towards cost saving initiatives, especially when rationalized applications are moved to the cloud. Gartner (2012) on the other hand estimated that by 2015, there will be a market volume of 22.1 billion USD and an estimated annual compound growth of 17.2% for 2012-2015 for on-demand applications.

Cloud computing strains many existing IT management and governance paradigms just as previous emerging technology trends have. As many organizations continue to adopt cloud computing for the various values it offers, the Cloud governance issues will become increasingly critical, especially in the areas of security, risk, interoperability, portability, vendor lock-in and others (Agile Path, 2013). Therefore, successful cloud adoption requires elaborate cloud governance. This involves defining policies and implementing an organizational structure with well-defined roles for the responsibility of IT Management, business processes and applications as these elements are moved out of the traditional IT environment to cloud (Bailey & Becker, 2014).

1.2 Problem statement

The definitional characteristics of Cloud Computing, such as multi-tenancy, elasticity, resource sharing and on demand provisioning have the potential to complicate traditional IT operations (CSA, 2010). The business models of Cloud Computing encourage many tiers of providers and customers within a single virtual infrastructure, thus increasing the surface area for external attacks. There is no perimeter anymore, no firewalls at the Internet gateway stopping attackers from attacking other systems. Coordinating appropriate and efficient incident response without impacting continuity of operations for other customers or without violating laws and contractual agreements is not clear in cloud computing environments. More importantly, most organizations have not tailored their IT processes like incident management, event management, problem management and change management processes for the cloud services. Instant access to cloud computing with direct access to the provider may allow governance processes to be bypassed, and this exposes the organization to various risks.

Many cloud consumers have extended their IT governance frameworks to their cloud services; however, these frameworks don't adequately address governance challenges in cloud environments. Additionally, most consumers don't have quantitative mechanisms to measure their cloud computing governance maturity, and therefore find it difficult to identify the opportunities to improve their cloud governance frameworks to attain a higher maturity level.

1.3 Research Objectives

The objectives of this research were:-

1. Identify the opportunities and challenges of cloud computing in organization.
2. To determine the various factors that contribute to and the extent to which they influence effective cloud computing governance
3. To develop a methodology to assess cloud governance readiness
4. To use the developed methodology to assess the cloud computing governance readiness of a local airline company

1.4 Significance of the study

Cloud governance remains a challenge to many organizations that have adopted cloud computing. Many of these organizations have extended their traditional on-premise IT governance processes to the cloud services. However, a methodology to evaluate cloud governance readiness is still lacking. This research developed a methodology to assess cloud governance readiness by studying the cloud governance practices in an airline company in Kenya. This proposed methodology will benefit other cloud computing consumers; both the current and potential by providing recommendations on how to improve governance practices to attain the highest maturity level of cloud governance readiness. Additionally, it will open room for further research regarding cloud computing governance. It will also help cloud service providers to improve their services to meet and even exceed their client expectations.

1.5 Research Question

1. What are the major opportunities offered by cloud computing and the challenges it presents to the organization?
2. What processes has the organization implemented to support cloud computing governance and to how extent do they contribute towards effective cloud governance?
3. How cloud governance ready is the organization?
4. How can these processes be improved to ensure the organization attains the highest cloud governance readiness level?

1.6 Chapter Summary

Chapter 1: Introduction

This chapter has presented the problem that this research purposed to address, by highlighting the challenges organizations face in assessing cloud governance readiness. It has presented the key objectives of the research, the research questions that the research has answered regarding cloud computing governance, as well as the significance of the research to both the industry practitioners and academic researchers.

Chapter 2: Literature Review

This chapter reviewed other literature on cloud computing governance. It highlighted the various definitions of cloud computing and cloud governance. It also summarized the various service models and deployment models of cloud computing. It further looked at the various cloud governance models that have been proposed by various industry players and academic researchers. This research identified Saidah and Abdelbaki model as the most suitable cloud governance model. From the literature review, a conceptual model was developed, upon which this research was based.

Chapter 3: Research Methodology

The chapter focused mainly on the research methodology. This research used both Quantitative and qualitative research approaches. Quantitative data was collected through online questionnaires while qualitative data was collected through Focus Group Discussion (FGD). The research design, population and sampling techniques were also discussed in this chapter. Finally the chapter discussed the analysis methods. Quantitative data was analyzed using SPSS statistical software to perform path analysis, which generated the correlation between the dependent variable and the independent variables. This was presented in terms of *beta* correlation and *alpha* correlation co-efficients. For qualitative data, the FGD results were coded and sorted based on the themes developed. The data was therefore analyzed on the basis of frequency and percentages.

Chapter 4: Results and Discussions

The chapter presented the results of both qualitative and quantitative results. The results validated the conceptual framework by comparing the *alpha* correlation co-efficient values with the significant value of 0.05. Those that are less than 0.05 were marked as supported while those greater than this value were marked as not supported initial. From these results, the conceptual model was then reviewed, with only those that are supported appearing in the model.

Finally, this chapter aggregated the *beta* co-efficient values and compared the sum with the class limits of a scale developed in the methodology to rate the organization on the scale. The sum of

the beta co-efficients was found to be within the upper and lower limits of the initial cloud governance maturity level.

Chapter 5: Conclusions and Recommendations

This chapter gave conclusions and recommendations based on the results in the previous chapter. From the research results, it has been concluded that the organization has insufficient security controls for the cloud services, it's not clear who bears encryption key management responsibility, there is no visibility into the backup location thus the risk of hosting company data in proscribed locations, exit policy is not clear and inadequate human resources to manage cloud services. Based on those conclusions, the research recommended proper identity management policies, clear definition of encryption key management responsibility, full disclosure of backup and recovery locations, clear exit policy and resource management as the most important measures that will help the organization to attain the highest level of cloud governance maturity level.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

This chapter presents a collection of topics which are relevant to this study. These topics include definitions of cloud computing, cloud computing services, cloud development models, evolution of cloud computing, benefits of cloud computing, key cloud technologies, key characteristics of cloud computing, cloud readiness models and cloud adaptation models.

The purpose of this chapter is to analyze recently published works on cloud computing in order to gather the most recently and significant data and give the weight to this study.

2.1 Cloud Computing

As a new paradigm in Information Technology, cloud computing has attracted great interest both in research and practice (Loebbecke and Ullrich, 2011). Cloud computing has been defined by various institutions and individuals, including Gartner, Forrester, IDC, NIST and communications of the ACM.

National institute of standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services)that can be rapidly provisioned and released with minimal management effort or cloud provider interaction" (IT Laboratory-NIST).

According to Abadi (2009), cloud computing involves delivery of IT services throughout a network such as the internet. Seaten (2008) a principal Analyst at Forrester defines cloud computing as a standardized IT capabilities (services, software or infrastructure) delivered via internet technologies in a pay-per-use, self-service way.

Enterprise Strategy Group (2009) stresses on the concept of metering of the services by defining cloud computing as a service model where business workloads are deployed on the internet and the business pays for what has been consumed. Gartner defines cloud computing as a computing model where scalable and elastic IT-enabled capabilities are delivered over the internet as a service. This definition emphasizes on scalability and elasticity characteristics of cloud computing.

In conclusion, many researchers and institutions have tried to define cloud computing in different ways; however, as observed by Green (2009), many agree that cloud computing is a shift from traditional computing in terms of storage location, hardware ownership, software delivery, interfaces to other systems, business processes, and personal collaboration. It is therefore difficult to pint-point a single definition as the best definition. Based on the scope and objectives of this research, the NIST definition of cloud computing will be adopted.

2.1.1. Characteristics of Cloud Computing Models

Dallas Chapter of Institute of Internal Auditors (2012) identified the following characteristics of cloud computing:-

i. On-demand self-service:- unilateral provisioning of compute resources (i.e. server time and network storage) is performed automatically, without human interaction with a service provider.
ii. Broad network access: - there is anywhere and anytime access to the cloud services via internet via thin or thick client platforms, such as mobile phones, tablets, laptops, and workstations.
iii. Resource pooling: - cloud computing involves multi-tenancy where multiple consumers are served, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
iv. Rapid elasticity: - the compute resources can be automatically scaled in and out, up and down commensurate with demand.
v. Measured service: - Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service (Grance & Mell, 2011).

2.1.2. Cloud services Delivery Models

i. **Infrastructure as a Service (IaaS):-** this is a service model where provisioning of compute resources (e.g., processing, storage, networks) is done over the internet (NIST, 2010). Ramesh et al. (2014) describe this as a model where cloud service provider provides the resources to the client on demand basis from their data centers. Giovanoli (2011) drew similarity between IaaS and SaaS stating that both involve provision of services on demand through the internet.

ii. **Platform as a Service (Paas)**:-this cloud service model involves provisioning the capability to deploy applications developed by the user to the cloud, with provider-supported programming languages and tools. Ramesh et al. (2014) further stated that these resources are provided to the user by the cloud service provider on demand basis from their data centers.

iii. **Software as a Service (SaaS)**:- this is a service delivery model where the client is provided with access to a provider's software applications running on a cloud infrastructure. Ramesh et al. (2014) describe SaaS as a service model where users are provided access to software applications and databases. Ramesh et al. give an alternative name to SaaS as "On-Demand Software Services". Security Management, availability, and performance of a SaaS application is vendor-Managed (Salesforge, 2009). Choundhary (2007) estimated SaaS growth to be 50% per year.

2.1.3. Cloud implementation models

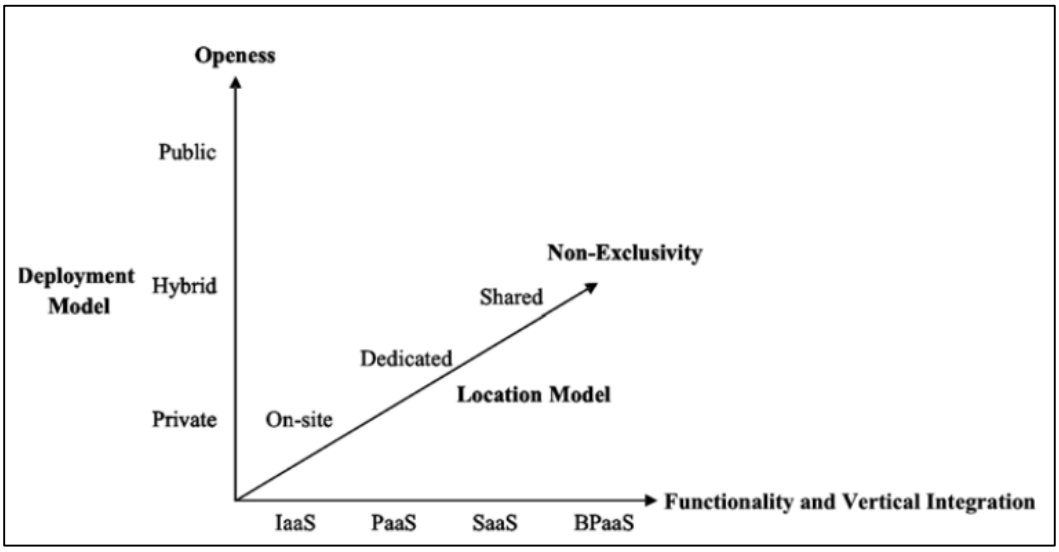
i. **Private Cloud:** This is a cloud deployment model where infrastructure is owned by a single organization. In this model, the organization maintains their own auditing principles and processes (Ramesh et al., 2014). As stated by Ramesh et al., private clouds don't connect to other clouds on the internet; therefore there are lesser chances of external attacks. As opposed to public clouds, private clouds allows individualization of the services by allowing customized configuration and implementation of services to suit business processes and needs (Giovanoli, 2011).

ii. **Public Cloud: -** this is a cloud deployment model where the services are available on public networks and is open for public access (Ramesh et. al, 2014). As opposed to private cloud, this cloud deployment model allows connection to other clouds, and what limits the number of users who connect to this cloud is mainly service provider's capacity (He, 2011). Ramesh et al. (2014) identified Service Level Agreement (SLA) management as the major challenge in public cloud management, stating that there's less transparency between the service provider and the cloud user in terms of SLA and this increases chances of violation.

iii. **Community cloud: -** this cloud implementation belongs to several organizations, who share infrastructure. The infrastructure is managed internally by the organizations or by a contracted third party (He, 2011).

iv. **Hybrid cloud: -** this deployment model combines two or more Private, Public and Community clouds. For successful deployment of hybrid cloud, interface barriers, middleware and standard barriers must be addressed (BITKOM, 2009). Integration of heterogeneous interface cloud environments of different companies and third-party vendors diverging to a homogenous interface for the end users must possible for successful implementation of hybrid clouds. Finally, the vendor must win client's trust in terms of data security and compliance for successful hybrid cloud implementation. Huthmacher (2010) stated that hybrid cloud provides the possibility to deploy the applications with important security or legal concerns in a private cloud and others not limited by security or legal concerns applications can be hosted by a cloud provider. Huthmacher identifies the major challenge in hybrid cloud as integrated implementation of a traditional IT environment with the public and or private cloud.

Figure 1: Cloud computing service models vs. Deployment Models



Source: Thomas & Ullrich (2011)

2.2 Cloud Computing in Aviation Industry

Mercator (2015) observed that as cloud computing gains prominence, the opportunity for airlines to build brand value, better service and understand customers, and drive excellence with cloud projects has become a reality. However, as Mercator observes, airline industry that has always been an early adopter of cutting edge IT solutions has become cautious when it comes to cloud computing.

HCL (2012) states that a move to cloud computing has the potential to not only simplify and accelerate business processes but also generate growth with faster product and services innovation, greater flexibility to react to increased demands and improved business intelligence and reduced costs. HCL identifies the potential benefits of cloud computing in Airline industry as real-time analytics and business intelligence, higher customer experience, cost savings with focus on core services and security. As observed by Blaisdell, airlines are struggling with huge quantities of data in complex environments, and global staff require 24/7 access to data in order to keep ground and air operations running seamlessly. He notes that cloud computing has already been adopted by many airlines, and cites a case where it helped advance the status of the black box in terms of investigation after Air Asia flight QZ8501 incident (Blaisdell, 2015).

Airline IT Trends Survey (2012) states that 75% of airlines plan to implement infrastructure-as-a-service technology by 2015 and a similar number plan to implement Software–as-a-Service. The study also states that nearly 40% of airlines are already using SaaS. Finally, the study states that almost 70% of airlines surveyed indicated that they plan to use desktop-as-a-service technology by 2015, though only 11% already have this service up and running.

2.3 Cloud Governance

Cloud governance is part of IT governance, which is a subset of corporate governance. Saidah & Abdelbaki (2014) define cloud governance as a framework applied to all related parties and business processes in a secure way, to guarantee that the organization's Cloud supports the goals of organization strategies and objectives. Corporate governance is a set of processes, customs, policies, laws and institutions affecting the way in which a corporation is directed, administered or controlled (De Leusse, Dimitrakos & Brossard, 2009). Corporate governance involves establishing chain of responsibilities, authority, and communication to empower people (decision rights), as well as establishing measurement, policy and control mechanisms to enable people to carry out their roles and responsibilities.

As part of corporate governance, IT governance that pertains to IT processes and supports the goal of business in an organization (He, 2011). He (2011) defines cloud governance as a framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensure that the organization’s cloud capability supports and enables the achievement of its strategies and objectives.

COBIT (2005) defines IT governance as decision rights, accountability framework and processes to encourage desirable behavior in the use of IT. This research adopts COBIT definition of cloud governance by COBIT.

Deliverables of IT governance includes business growth, cost effectiveness, asset utilization, and business agility (Weill & Ross, 2004). Weill & Ross state that these deliverables help organizations in strategically aligning business with the business. As organizations strive to adopt cloud computing for its various offerings, IT governance needs to be integrated to ensure full benefits of cloud deployments.

Dreyfuss (2009) observed that the new cloud environment is very different from traditional outsourcing and requires a new approach to governance and management. Some organizations nave extended their existing governance practices to their cloud services; however, as observed by Bailey & Becker (2014), extending governance to the cloud further complicates delivery of effective IT governance. Mangiuc (2001) identifies control of the service provider on the management of the cloud environment and some areas of business process as a major challenge to IT governance in cloud. Bailey & Becker (2009) noted despite the many benefits cloud computing offers, it introduces new challenges which should be considered before making any migration efforts to cloud. These issues were identified as internal threats (standards, controls, interfaces, handoffs and integration requirements), horizontal audit compliance, performance metrics which provide a quantifiable assessment of successful cloud resource integration, security and accountability and responsibility. Bailey & Becker suggested that a practical governance framework should be implemented and sustained in order to derive value from cloud computing investments. Mimecast (2009) established that among 565 IT managers interviewed across US and Canada, 62% have considered or are considering moving to cloud. However, most organizations are concerned about security, privacy, location of cloud services and compliance (Armbrust, et al. 2009; Dillon, Chen & Chang, 2010; Kumar, 2012). In order to address these challenges with cloud computing, various researchers have suggested the adoption of cloud governance (Guo, Song & Song, 2010; O'Neill, 2009; He, 2011). Some of these challenges, which are mostly governance related, have been identified by He (2011) as presented in table 1.

Table 1: Challenges of cloud Computing Governance

Category	**Description**
Compliance to laws and standards	• Locations of the services/data are need to control to ensure they are compliant to legal and business regulations.
Hard to estimate the risks of cloud computing	• Companies do not hold a holistic view of risk regarding cloud computing and lack of approach to assess those risks
Consequences of changing services	• Change of service will incur unexpected results if dependency of services or components is not well defined and recorded. • Unexpected access service and change service will cause major business loss.
Ensuring quality of the services	• Quality of the services such as performance, availability and security of the services are needed to carefully monitor to ensure the business value, especially when the services are out of control of organizations. • Lack of testing capability regarding cloud services. • Lack of capability to monitor composite services from different sources/CSPs, it becomes more complex when services are outside boundary of organizations.
Aligning cloud computing objectives with business objectives	• Aligning organizations with strategic goals is not changed in cloud setting. • Changes on how services are charged and how costs are allocated within the organization; funding models is moving from project-based to pool-based. • Inability to identify which service should move to cloud. • Inability to determine when to add/remove cloud services.
Cooperation with suppliers	• Empower roles and responsibilities to facilitate the cloud computing adoption might be emergent. • Communication requires aligning with current existing business unit as well as IT experts on the field.

Evaluate Cloud Service Providers	• Evaluate the processes and policies which the service providers define to ensure the consistence with internal service and security processes with the organization. • Ensure that CSPs have put the privacy control in place and demonstrate the ability to prevent, detect, and react to the breaches in timely manner. • Ensure that CSPs have the effective and robust security controls assuring information from their consumers. Ensure that the organization can rely on the controls to secure against the unauthorized access, change and destruction. • Ensure that CSPs are doing the "right" thing through third party certification such as third-party or service audit reports.

Source: He (2011)

The various cloud computing challenges can be classified under service governance, organizational change and strategic alignment challenges (Linthicum, 2009; Nadhan, 2004; Progress Software, 2005; Schepers, 2007).

Some researchers argue that Service Oriented Architecture (SOA) governance can be adopted for cloud computing (He, 2011; de Leusse, et al., 2009; Linthicum, 2009; O'Neill, 2009). He (2011) states that SOA governance makes changes from IT governance to ensure that the concepts and principles for service orientation architecture are managed appropriately and that the services are developed to meet the business goals.

However, some researchers have been able to distinguish between SOA and cloud governance, identifying both similarities and differences between the two. The first similarity drawn between SOA and cloud governance is that both require moving away from looking at IT usage from individual business units to the overall business requirements (Ovum, 2010). Another similarity between SOA and cloud governance is service governance, for instance, life cycle management of service, design time, runtime and change management (He, 2011; Linthicum, 2009; O'Neill, 2009). Both SOA and cloud governance require a new cost allocation model for service within the organization (Bentley, 2010), are process-oriented (O'Neill, 2009), both require dependency

management (Ovum, 2010), and both rely on policy to ensure the compliance of services to established standards. The differences between SOA and cloud governance have been summarized in table 2 below:

Table 2: Differences between SOA and Cloud Governance

SOA Governance	**Cloud Governance**
The platform service (Service-Oriented Infrastructure): delivers the hardware and software foundation such as server, network, database, operating system, clustering/grid/virtualization etc. on which software components run but are abstracted from.	IaaS and PaaS have been designed on the basis of SOA principles (Ovum, 2010)
The application/process service level: refers to software-only services.	Many SaaS applications have been designed on the basis of SOA principles. (Ovum, 2010)
SOA emphasizes on managing assets first, enforcement and monitoring second	Cloud demands organizations to address enforcement and monitoring first.
SOA doesn't emphasize on scalability, high performance and multi-tenancy	Cloud computing emphasizes on scalability, high performance1 (e.g. resource pooling) and multi-tenant (Yi & Blake, 2010)

Source: He (2011)

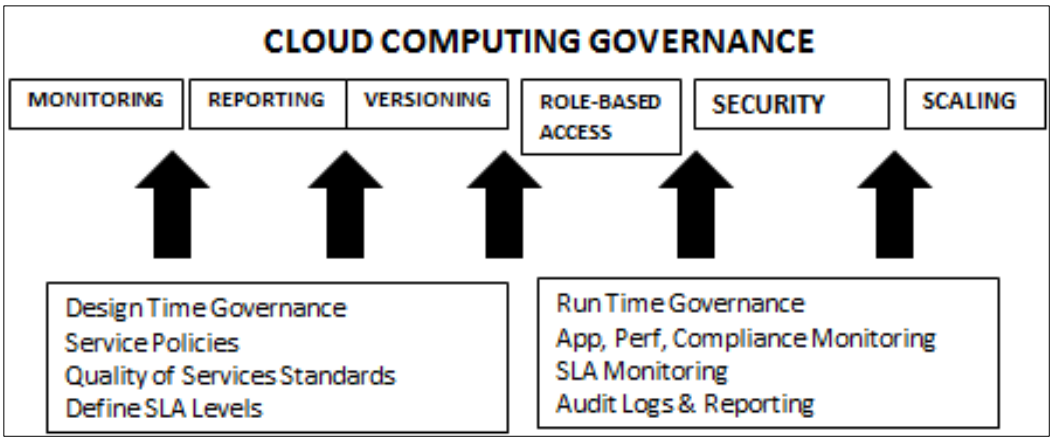
2.4 Cloud Governance Models

This section discusses the various cloud governance models by identifying their strengths and weaknesses.

2.4.1. Microsoft's Cloud Governance Model

Microsoft Cloud Governance Model's major focus is policy management and was developed for Windows Azure cloud platform (Microsoft, 2010). This model has three main components, namely design time (defines service policies, quality of standards and SLAs), run time governance (policies enforced and application or service performance and compliance are carefully monitored), and change management governance (tracks the change activities and assets; provide and manage report, alert, and log). As He (2011) stated, these three components are work in an integrated manner to ensure correct versioning, scale and ensure security compliance.

Figure2: Microsoft's Cloud Governance Model



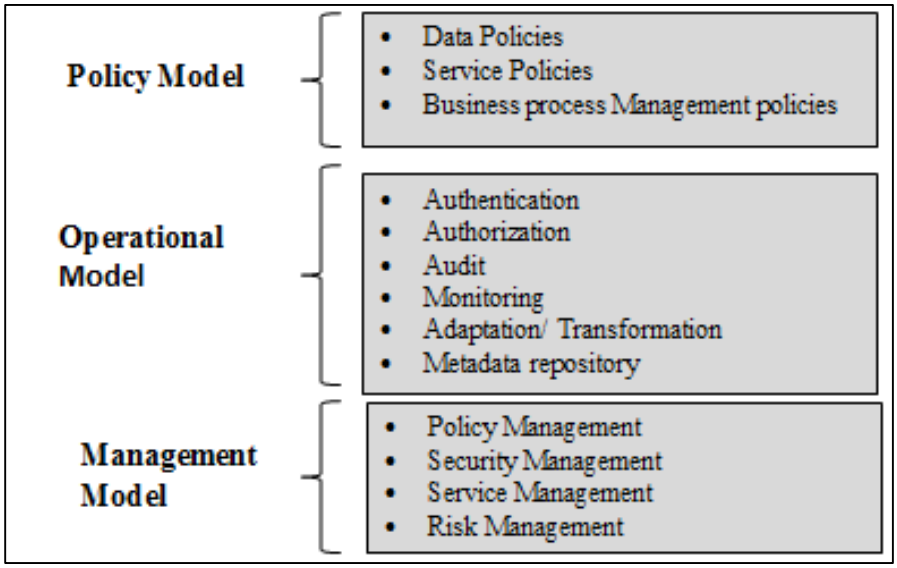
Source: Microsoft, 2010

This model comprehensively covers the technical aspects of governance. It adequately defines security, scalability, versioning, access and monitoring of cloud services. Furthermore, it separates design time governance from run time governance, therefore minimizes the chances of the governance elements being ignored at any of those stages. This model however doesn't address the alignment of IT and the business (He, 2011), which is a key cloud governance component. It also lacks exit strategy, which is key in managing cloud services.

2.4.2. Guo's Cloud Governance Model

This model has been identified by various researchers as the first proposed academic model for cloud governance (He, 2011; Saidah &Abdelbaki, 2014). It discusses the aspects of cloud governance in general (He, 2011).It was created based on four objectives of cloud governance, security, policy, and risk and compliance management. Guo's model classifies the components of cloud governance into three categories; policy, operational and management activities.

Figure3: Cloud Governance Model from Guo et al.



Source: Guo, et al., 2010

Several gaps have been identified in this model by various researchers. This model ignores IT and organizational alignment, which devalues the introduction of cloud computing (He, 2011; Saidah & Abdelbaki, 2014). Saidah & Abdelbaki also noted that this model lacks a feedback mechanism, which is necessary to improve efficiency and reliability of cloud services. Another important aspect missing in this model is asset management, which is a key component of IT governance (Saidah & Abdelbaki, 2014). Finally, Guo's model lacks and exit strategy, therefore there's no clear end of contract management, data and system maintenance in this model.

2.4.3. Saidah & Abdelbaki Model

Saidah & Abdelbaki (2014) stated that cloud governance process guarantees the rights of all stakeholders. However, they acknowledge that the challenge is the trade-off to achieve a governance model's implementation plan agreed by all parties. They therefore suggest that an elastic and customizable model to all models and business cases. They further suggest that the plan has to tolerate moving between the service providers and their customers.

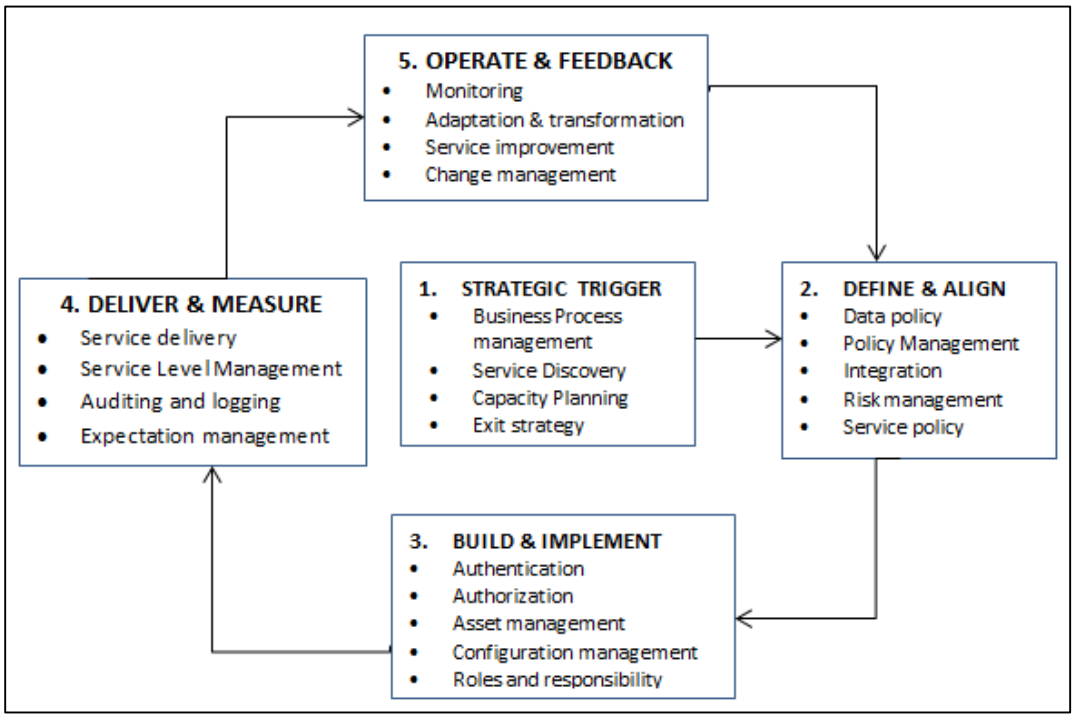
In their model, Saidah & Abdelbaki distributed controls under each model and its components to illustrate the practical implementation of governance. This model categorizes the controls into two main categories; normal controls and key controls.

This model is based on Guo's model, however, it tries to bridge the gaps identified in Guo's model by redefining the three components (policy, operational and management) to be processes. New processes are then created for the controls that are not relevant to any existing process. It further improves Guo's model by clearly defining the roles and responsibilities under the security management. This is helpful in aligning cloud system roles with the organizations roles and responsibilities. Additionally, they have added service improvement to the service management to be used as a key to feedback to increase system reliability and efficiency.

Under operational model, they define the asset management, configuration management and capacity planning. Finally, exit strategy has been added to in this model, which should be defined in any contract separately to define the procedures to be done to maintain user systems and data after ending the cloud service or moving to a new provider.

This model has five stages namely strategic trigger, define and align, build and implement, deliver and measure, and finally operate and feedback. This model addresses the lack of feedback in Guo's model by introducing service improvement to service management to be used as a key of the feedback to increase system reliability and efficiency.

Figure 4: Saidah & Abdelbaki Cloud Governance Model



Source: Saidah, A & Abdelbaki, N, 2014

Strategic Trigger is the event that initiates the need for cloud computing. Usually, business need is the main trigger for using cloud services. It has four processes. Business Process management policy which defines interrelations between cloud-based services, Service discovery finds and discovers the existing services and available technologies for new services, Capacity planning reviews the existing environment and future business extensions to plan the best way technically and financially to achieve business goals, Exit strategy addresses the need to change from one service provider to another. Exit strategy is mandatory in this stage.

Define and align is the second stage of cloud computing adoption or transformation of an existing environment to cloud. This stage ensures strategic alignment of cloud computing objectives with the overall business objectives. It has six processes; data policy which defines data's physical and logical model, service policy which builds a service dictionary by defining integration and

separation of the service based on the deployment model, Policy management determines and reviews the cloud service policy, Risk management which identifies the various risks and their mitigation measures. Integration policy which defines integration of existing infrastructure with cloud infrastructure is a mandatory process if an infrastructure already exists. Build and implement stage addresses issues related to people, processes and infrastructure technology. This stage contains eight processes; authentication, authorization, metadata repository, asset management, configuration management, roles and responsibility, privacy and access.

Deliver and measure stage ensures alignment of the implemented cloud services with the planned services. This stage measures and compares the outputs with the targets. It contains four processes; service delivery which involves moving the service to the execution environment, SLA management which ensures that the agreed service levels are met, errors and expectation management which reviews the current environment with analyzes the running systems and reports the existing errors, auditing and logging track all the activities and define whom, when and where an activity was performed.

The final stage of this model is operate and feedback which contains four processes; Monitoring which collects transaction and access data to present a service statistics, adaptation and transformation manages the unavoidable consequences and changes in the running services, service improvement assesses measures and improves everything in the system, change management which transforms the service to a desired future state.

This model is quite comprehensive and covers most cloud governance in details. This research used this model since it comprehensively covers all the dependent and independent variables that are key to this study.

Table 3: Operational definition of the model terms

Model	**Terminology**	**Operational Definition**
Policy Model	Data Policy	Refers to the regulations governing an organizations data during transit to the cloud as well as the data that's already residing in the cloud environment.
	Service Policy	This is a policy that enforces an understanding of the client requirements among the service providers.
	Business Process Management Policy	This is a policy that governs the systematic approach to making an organization's workflow more effective, more efficient and more capable of adapting to an ever-changing environment
	Exit Policy	This refers to the regulation regarding decommissioning/ retiring of a cloud service. This may involve the procedure to be followed in migrating a service back to an organization's premises.
Operational Model	Authentication	Refers to the process of verifying the identity of a user by obtaining some sort of credentials and using those credentials to verify the user's identity in a cloud environment
	Authorization	Refers to the process of verifying that you have access to something in the cloud environment.
	Audit	Refers to is a specification for the presentation of information about how a cloud computing service provider addresses control frameworks
	Monitoring	Refers to regular observation and recording of activities taking place in a cloud environment.
	Adaptation/ Transformation	
	Meta data repository	This refers to a repository containing data about the data stored in the cloud.
	Asset Management	Involves acquiring and maintaining both human and computing resources in cloud computing environment

	Configuration Management & documentation	Refers to the process of establishing and maintaining consistency of a cloud service performance, functional and physical attributes with its requirements, design and operational information throughout its life.
	Capacity planning	Refers to the process of estimating the resource requirement in cloud environment that will be needed over some future period of time.
Management Model	Policy Management	Refers to the process of developing and maintaining a set of policies to support an organizations' cloud policy strategy.
	Security Management	Refers to a set of policies concerned with information security management or IT related risks.
	Service Management	Refers to strategic approach to designing, delivering, managing and improving the way a cloud service is used within an organization.
	Risk Management	Refers to how the risks associated with cloud computing are identified and reduced to acceptable levels.
	Change Management	Refers to how changes approved and tracked before application to the production cloud environment.

Source: Research

2.5 Cloud Computing-Capability Maturity Model

According to Schmidt & Grabski (2014), Cloud Computing-Capability Maturity Model is based on Software Engineering Institute's Capability Maturity Model (CMM), which is a well-established process improvement model. CMM has provided foundation for development of a number of capability models. General CCM approach is to define a series of increasing capability levels by which to assess an organization processes, job assignments, organization structures, measures and innovativeness (Schmidt & Grabski, 2014).

IT-Capability Maturity Framework (IT-MCF), on which Schmidt & Grabski (2014) quotes Curley et al (2012) as establishing an archetype of the maturity level of an organization as it implements, improves and controls IT capabilities to support organizational value creation. Schmidt & Grabski (2014) stated that IT-CMF is designed as a high-level framework that's application across the organizations and might not fully capture nuanced differences that result from changes in technology, business processes and governance. This therefore necessitated them to propose a cloud Computing Capability Maturity Model (CC-CMM), which according to Schmidt & Grabski allows for flexibility and variation, needed when dealing with the emerging cloud computing issues and environment which wouldn't be present in a static framework. CC-CMM addresses risk and assurance issues. The risks associated with cloud governance should be evaluated based upon strategic alignment, risks exposures created by use of cloud services, management of all corporate IT assets, and the manner in which the CSP performance will be evaluated in terms of service level management (Henhall, 2010).

Schmidt & Grabski (2014) identify the specific factors to be considered as:-

a) Level of management control and audit visibility into cloud
b) CSP internal controls
c) Independent audit of the CSP, for example SSAE 16 and ISAE 3402.

Schmidt & Grabski conclude that since critical applications may be placed in the cloud, risk assessments, controls and assurance, and operational service level agreements and plans for external auditing need to be a key component of the initial cloud computing planning and contracting process.

CC-CMM contains 3 dimensions:-

a) CCM Levels
b) Cloud Computing Capability areas

c) Cloud Computing types

Maturity Levels

CC-CMM proposes 5 maturity levels, building on Yeo and Ren (2009) whose maturity model is based on Software Engineering CMM.

i. *Level 1&2:* Organizations haven't addressed risks associated with cloud computing

ii. *Level 3:* this has been termed as demarcation level by Schmidt & Grabski. At this level, the organization has formalized assessment of cloud computing risk management. The risk management process is understood throughout the organization.

iii. *Level 4&5:* At these two levels, the organization includes and acknowledges key external stakeholders; both direct and indirect CSPs, for instance SaaS provider and IaaS provider used by SaaS. The organization also develops continuous process improvement.

Table 4: Cloud Computing Capability Maturity Levels

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

Source: Schmidt & Grabski

Cloud Computing Capability Areas

Schmidt & Grabski identifies six cloud computing capability areas based on COBIT 5. These areas include IT governance, management, data governance, security reliability, software applications and technical.

i. *IT Governance:* - Schmidt & Grabski state that shared governance is needed because it's possible and even likely that IT decision rights migrate outside of the organization to the CSP. Rittenberg & Martens (2012) state that an organization must determine its risk appetite and overall enterprise risk management (ERM) approach.

ii. *Management:* - Schmidt & Grabski quote Badger et al (2012) that management capabilities are based upon the general recommendations for cloud computing. Schmidt & Grabski (2012) says that this should include specification of how data will be migrated to and from the cloud. This also includes data retrieval plans, CSP's plans for continuity of operations and redundancy plans, SLAs that specify remediation in case failure, CSP's compliance with controls (through third party audits) and assurance that CSP has appropriate internal controls over their administration staff to prevent any type of security lapse. Acceptable use policy must be reviewed and vetted, along with inclusion of any needed modifications.

iii. *Data Governance:* - this includes security, integrity and access to data placed in the cloud. Data movement and storage may be restricted by regulatory issues and government contracts. Other considerations in data governance include how and where data is stored, assurance of data deletion upon exit, determination of who is responsible for backups and restores and data archiving policy.

iv. *Security and reliability:*- this ensures that only the organization's specified users can access the data and that the CSP is able to provide the agreed upon services based upon the originally specified performance parameters. Security includes encryption, physical security, authentication, and IAM techniques. Performance capabilities include specification of performance benchmarks or other Key performance Indicators (KPIs) and gaining visibility into the CSP's operations as far as an organization's data is concerned.

v. *Software and applications:* - this addresses differences between the application types, that an organization might place into the cloud, and the required performance levels and required support.

vi. *Technical:-*this focuses on the use of virtual machines. An organization must ensure that the CSP can both protect against and detect attacks from other virtual machines or other sources. Organizations should also be able to move from one set of virtual machines with one CSP to another, or back to the premises.

Cloud Computing Types

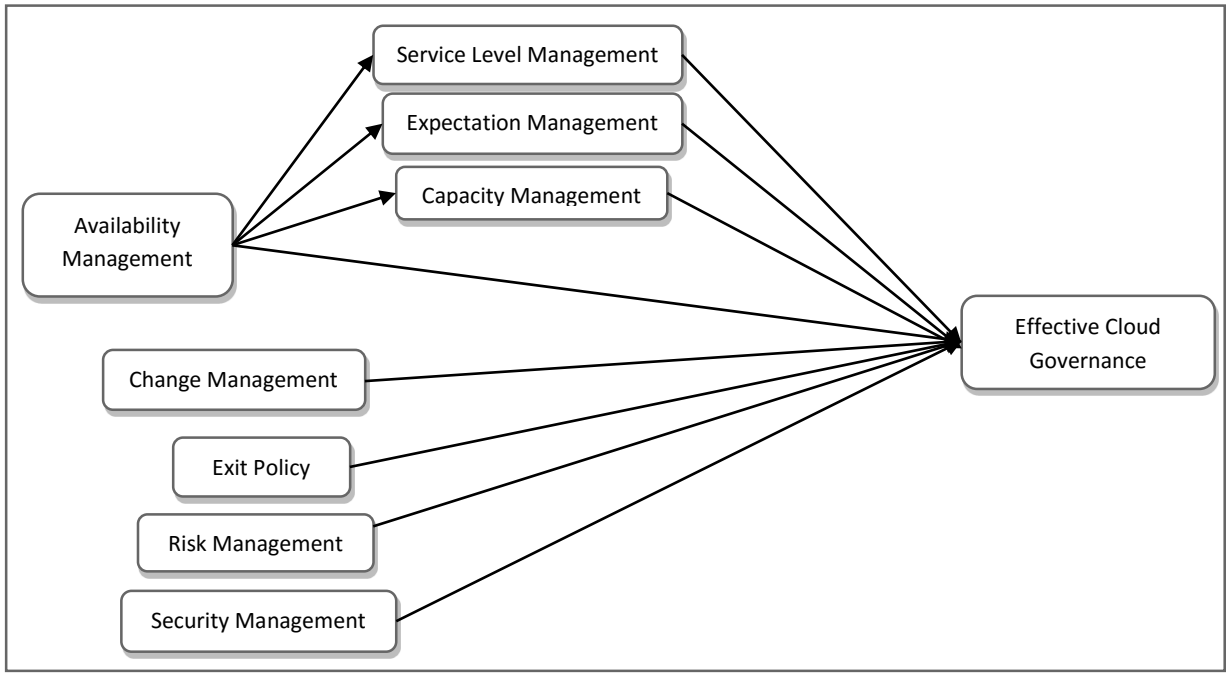
This includes the various cloud service models (IaaS, PaaS and SaaS) that have been discussed in details in section 2.2.2.

2.6 Conceptual Model

In order to determine the weights to different research variables that will be used for cloud governance readiness assessment, the research modified Saidah & Abdelbaki model to come up with a conceptual model for this study. The resultant conceptual model is a causal relationship among the dependent and the independent variables. In the conceptual model, only the processes that are important to this study has been used as variables. The direction of the arrow in this model shows an element causal effect of the variables, with the arrow pointing towards the effect. The components of this model were used to generate the questions for the research questionnaire for both qualitative and quantitative data collected. In addition, some general questions were added to the questionnaire to capture the demographics and the various cloud computing service models and deployment models implemented by the organization.

Causal Relationship between variables

Figure 5: Conceptual Model



Source: Research

2.7 Research Hypotheses

To test the conceptual model, the following hypotheses were proposed:

H1: Existence of a Cloud computing Availability Management process has a direct positive impact on Effective Cloud Governance

ISO/IEC 20000- 1:2005 IT Service Management - Specification (2005) states that the CSP must ensure that agreed service continuity and availability commitments to customers can be met in all circumstances. To meet these requirements, there must be a formal monitoring and recording of availability as well as a service continuity plan (Ristola, 2010). Ristola further states that the service continuity plans and availability management process need to be considered in the change management process so that changes in any part of the system re updated in all the relevant places.

H2: Proper Service Level Management results into Effective Cloud Governance

Axelos (2014) defines service in cloud computing context as "providing value to customers by facilitating outcomes customers want to achieve without ownership of specific costs and risks". Service delivery must be measured across virtualized delivery so that individual services and overall cloud infrastructure

can be measured (Enterprise Management Associates, 2012). As observed by Jansen (2012), Service Level Management is very important for cloud services. Jansen further suggests that the Service Level Agreements (SLA) need to clearly define the responsibilities in service level management. He further adds that the relevance of underpinning contracts (UCs) should be considered.

As noted by Axelos, even though it's common for customers and consumers to expect higher levels of service than that provided by traditional IT service providers and internal IT organizations, these service levels may not be open for discussion or negotiation with the customer, thus it's important for customers to understand if they can define the levels of service quality and assurance they require in a negotiated Service Level Agreement. Axelos gives the following reasons for customers and consumers expectation of higher levels of service:

i. Loss of custody of data to cloud service provider, thus must be managed securely
ii. Security concerns due to increased exposure to external attacks
iii. Availability requirements
iv. Service continuity requirements
v. Fear, uncertainty and doubt
vi. Impact on public image regarding cloud computing reported in the public domain.

H3: Existence of Expectation Management process for cloud services is significant for an Effective Cloud Governance

Understanding and meeting customer expectations is an important part of Service Management for every cloud service provider (Lichtenberger, 2013). As Lichtenberger observed, some of these expectations may at times conflict each other. Lichtenberger identified cost versus quality and stability versus flexibility as some of conflicting expectation pairs. Lichtenberger therefore suggests trade-offs among the conflicting expectations so that the customer cloud computing expectations can be met.

H4: Cloud computing Capacity Management process is a recipe for an Effective Cloud Governance

According to ISO/IEC 20000- 1:2005 IT Service Management - Specification (2005), Capacity management ensures that the service provider has, at all times, sufficient capacity to meet the current and future agreed demands of the customer's business needs. Ristola (2010) observed that the customer and service specific capacity requirements are defined in the beginning of the customer relationship in the contract and the service descriptions. However, as Ristola observed, most cloud service customers have no process of evaluating and adjusting these plans after the initial agreement. He further notes that most clients are not aware or don't actively monitor the cloud service capacity levels.

H5: Effective cloud services Change Management policy enhances Effective Cloud Governance

ITIL V3 defines change management as the process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services. Axelos (2014) observes that change management process can be tailored to meet cloud computing requirements by adapting change management process to approve or decline additional SaaS subscriptions and adapting standard change requests to allow for certain cloud computing changes to be pre-approved.

H6: A clear cloud Exit Strategy is for Effective Cloud Governance

Exit policy which defines the process of terminating the use of a cloud service by a customer should be well defined (Cloud Standards Customer Council, 2013). CSCC further states that none of the customer's data should remain on the cloud platform when the customer has completed the termination process. As observed by CSCC, this is a shared responsibility between the customer and the service provider; the provider must ensure that all the customer data is deleted, including from the backup locations. On the other hand, the customer must ensure that they retrieve the data in a suitably secure form and ensure smooth transition without data loss. CSCC recommends a written confirmation from the provider to the customer that all data is deleted from the cloud platform and the process is complete.

CSCC recommends that the client evaluates the following when reviewing exit clause:

i. The amount of support provided by the cloud service provider and any financial implication of the support.
ii. Responsibility of removing data from the cloud platform lies on the provider, or the provider should assist the customer in extracting and erasing their data by providing clear and concise documentation.
iii. The format in which data is transmitted from provider to the customer should be specified in the Cloud Service Agreement, preferably in the standard data formats to ease and enhance portability.
iv. The retention policy after transition must be defined, after which the data will be completely removed.
v. Appropriate business continuity processes should be ensured by the customer during exit.
vi. Upon completion of the exit process, the provider should provide the customer with a written confirmation that data has been completely removed from the cloud platform and that the provider agrees not to use the customer data for any other reason in the future, including using the data for statistical purposes.

In conclusion, CSCC recommends that the customer undertakes due diligence when evaluating and selecting a cloud service provider. On the other hand, a trustworthy CSP should provide the customers with a fair and effective exit strategy.

H7: Risk Management policy for cloud services is important for Effective Cloud Governance

Risk is the possibility that an event will occur and adversely affect the achievement of objectives (COSO, 2004). COSO identified security, integrity, availability and performance as the possible types of risks that should be managed by a cloud consumer. COSO further identifies the following typical risks in cloud computing:-

i. Disruptive force: - facilitating innovation; with increased speed and the cost-savings aspects of cloud computing can themselves be viewed as risk events for some cloud consumers.
ii. Residing in the same risk ecosystem as the CPS and other tenants of the cloud
iii. Loss of custody of data to third-party, that is the cloud service providers
iv. Cloud service providers and their customer organizations are likely to have separate enterprise risk management (ERM) programs to address their respective universe of perceived risks.
v. Lack of transparency: – A CSP is unlikely to divulge detailed information about its processes, operations, controls, and methodologies.
vi. Reliability and performance issues: – System failure is a risk event that can occur in any computing environment but poses unique challenges with cloud computing.
vii. Vendor lock-in and lack of application portability or interoperability – Many CSPs offer application software development tools with their cloud solutions.
viii. Security and compliance concerns: – Depending on the processes cloud computing is supporting, security and retention issues can arise with respect to complying with regulations and laws such as the Sarbanes-Oxley Act of 2002 (SOX), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the various data privacy and protection regulations enacted in different countries.
ix. High-value cyber-attack targets: – The consolidation of multiple organizations operating on a CSP's infrastructure presents a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality and data integrity.
x. Risk of data leakage: – A multi-tenant cloud environment in which user organizations and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization. This risk of data leakage presents

an additional point of consideration with respect to meeting data privacy and confidentiality requirements.

These risks have to be managed for a cloud service consumer to get the expected value from their cloud investments.

H8: Security Management policy is necessary for an Effective Cloud Governance

According to ISO/IEC 20000- 1:2005 IT Service Management - Specification (2005), security management ensures that information security is effectively managed within all service activities. Jansen (2012) urges that a cloud consumer considers the boundary conditions, to ensure that private data of individuals are not stored in proscribed locations. Jansen also observed that the traditional security mechanisms like perimeter firewalls, demilitarized zones and intrusion detection systems don't work in cloud environment due to high level of virtualized nature of cloud infrastructures. However, Jansen states that some traditional security measures like server hardening and minimal installation of the operating system, user rights management and user data encryption are becoming more useful in securing cloud-based data.

CHAPTER 3: RESEARCH METHODOLOGY

3.0 Introduction

This chapter outlines the research methodology used in this research. This covers the research design, instrument design, population and sampling, data collection, data analysis and presentation methods. This research sought to establish the cloud governance readiness of a local airline through a conceptual model derived from Saidah & Abdelbaki. The primary constructs of this model include Availability Management, Change Management, Exit Strategy, Risk Management and Security Management as the independent variables. The dependent variable is effective cloud governance. Intervening variables in this research are Service Level Management, Expectation Management and Capacity Management.

3.1 Research Design

This study used mixed mode approach of both qualitative and quantitative methods. Additionally, this research was exploratory in nature. According to Merriam (2009), qualitative researchers are interested in understanding the meaning people have constructed, that is, how people make sense of their world and the experiences they have in the world. According to Parkinson & Drislane (2011), research using methods such as participant observation or case studies which result in a narrative, descriptive account of a setting or practice. Quantitative research on the other hand is a formal, objective, systematic process in which numerical data are used to obtain information about the world (Burns & Grove 2005).

The qualitative research provided in-depth explanations, respondent's experiences, opinion and knowledge while the quantitative research approach provided statistical data. Both techniques were used to draw from their strengths and minimize the weaknesses of quantitative and qualitative research approaches hence increase validity and reliability of the data collected.

3.2 Instrument design

Questionnaire was the major instrument for this study. The questionnaire questions were structured in a Likert scale format, with a scale of 1-5 (1: strongly disagree, 5: strongly agree). The questions in the Focus Group Discussion guide contained open-ended questions.

As observed by Burns and Grove (1993), questionnaires and interviews are almost the same, other than the fact that the questions in questionnaires tend to have less depth.

Questionnaire was chosen as the major instrument mainly because they are less time and energy consuming during administration, offers the possibility for anonymity therefore there was no fear of victimization on the respondents part, and they are easier to compare since most questions in this study will be close-ended.

However, Burns and Grove (2009) cautions that there is the question of validity and accuracy with the questionnaires. They add that the subjects might not reflect their true opinions but might answer what they think will please the researcher, as well as losing the value of information due to brevity of the answers. Interviews were carried out to complement these weaknesses.

In this research, the instrument and survey instruction were filed tested in advance of the actual data collection so that the potential problems and weaknesses could be identified as soon as possible. Field test of the survey questionnaire ensured validity of the measuring instrument and assured clarity of the questions to the respondents (Cooper & Schindler, 2008).

3.3 Population and sampling

The sampling frame for this study was a purposeful sample of the major cloud computing stakeholders in the organization. Purposive sampling involves an investigator selecting units that are representative or typical of the population, primarily relying on expert judgement or experiences of the unit (Singleton and Straits, 2005). The sampling frame for this study included 50 respondents from various sections in the airline.

Various literature offer methods and approaches of sample size determination, but there is no agreement on what the minimum sample size should be (Hailu, 2012). This survey used the formula suggested Yamane (1987) to calculate the sample size. The formula is:-

$$\mathbf{n} = \frac{\boldsymbol{N}}{\mathbf{1} + \boldsymbol{N}(\boldsymbol{e})^{\mathbf{2}}}$$

Where n is the sample size, **N** is the total population size, and **e** is the level of precision (sampling error). The minimum sample size for this study for a population, N of 50 respondents at 95% and with the degree of variability, **e** at 0.05 was calculated as:-

$$\mathbf{n} = \frac{\mathbf{50}}{\mathbf{1} + \mathbf{50}(\mathbf{0.05})^{\mathbf{2}}}$$

$$\mathbf{n} = \frac{\mathbf{50}}{\mathbf{1.125}}$$

$$\mathbf{n} = \mathbf{44}$$

This implies that a sample size of at least 44 respondents should be used for this survey to evaluate cloud governance readiness of the organization.

3.4 Data collection Procedure

The focus of study included the senior IT managers (including IT directors, IT security managers, MIS Managers), cloud computing using (systems analysts, systems administrator, systems developers and IT infrastructure specialists), and the business executives who participate in making IT related decisions. Questionnaires were administered to these respondents. These questionnaires were sent electronically using Google Forms. Some of these respondents were interviewed either face-to-face or through telephone.

According to the research schedule for this study, data collection was scheduled to take four weeks. The respondents to the survey study were anonymous mainly for ethical reasons. However, the response rate was actively monitored and assessed during the initial one week of the survey to determine the number and rate of responses and evaluate the progress.

The quality of survey response data submitted was checked to ensure accuracy, consistency across respondents, and to locate potential omissions or missing data. The data was checked and validated to ensure completeness and to prevent problems from occurring at the data analysis stage due to data collection error. This reduces errors in the recording, improves legibility, and clarifies unclear and inappropriate responses (Cooper & Schindler, 2008).

The data was collected mainly by distributing questionnaires to a focus group. Neuman (2009) argues that the purpose of focus group is to observe a wide range of ideas or feelings that people have about a phenomenon. This research used this data gathering methodology, where a group of participants was formed for the purpose of discussing the questionnaire questions. This group consisted five individuals with different roles regarding cloud computing.

3.4.1 Reliability and Validity

Reliability

Reliability is the degree of consistency with which an instrument measures the attribute it is designed for (Polit & Hungler, 1993). The researcher ensured standardized conditions such as exhibiting similar personal attributes to all the respondents.

The researcher booked prior appointment with the interviewees to ensure that the interview was carried out at a time convenient to both parties. The questionnaire respondents were given adequate

time to fill and return the questionnaires. Finally, confidentiality was ensured by encouraging the respondents who wish to be anonymous not to indicate their identities on the questionnaires.

Validity

Validity can be discussed from the instrument and content points of view. Validity of an instrument as the degree to which an instrument measures what it's intended to measure (Cooper & Schindler, 2008; Polit & Hungler, 1993). Creswell (2009) notes that validity indicates whether one can draw meaning and useful inferences from scores on the instrument. Polit & Hungler stated that content validity is the extent to which an instrument represents the factors under study.

There are two types of validity: external and internal validity. For quantitative studies, external validity is the extent to which the results of a research are generalized (Hailu, 2012). Hailu (2012) describes internal validity as the rigor of a study and the extent to which the designers have taken into account the explanation of any causal relationships the results may reveal.

Cooper and Schindler (2008) noted that field test of the survey questionnaire ensures content validity of the measuring instrument and assures clarity of the questions by participants as well as providing a general overview of the feasibility of the survey instrument including the duration for the completion of the survey. Creswell (2009) noted that the test makes the researcher aware of the potential problems that would arise from utilizing the survey instrument and help to improve the questions, instrument format and the scale.

Questionnaire questions were comprehensive to ensure that adequate information relevant to cloud computing governance was collected for analysis. These questions were formulated in a simple language, and the respondents were encouraged to seek clarification for the questions that seem unclear to them.

3.4.2 Field Test

According to Hailu (2012), the primary objective of field test is to validate the face validity, logical coherence, question integrity, readability, and appropriateness of the instrument. Creswell (2009) states that it is important to establish the content validity of an instrument and improve questions, format and the scales. Field test of the survey questionnaire ensures content validity of the measuring instrument and assured clarity of the questions by participants as well as providing a general overview of the feasibility of the survey instrument including the duration for the completion of the survey (Cooper & Schindler, 2008).

During the pre-test, the major weakness of the instrument identified was that it was too long and therefore respondents would be discouraged from filling it to completion. This therefore necessitated braking down the questionnaire into two; for cloud computing operations (meant for cloud technical staff), cloud computing policy management (meant for cloud computing policy makers). These were then sent to the relevant respondents, thus increasing the validity of the instrument.

The field test was done electronically over the internet by use of Google Forms.

3.5 Data Analysis

i. Qualitative Data Analysis

Using Microsoft Work for coding and retrieval of qualitative data involved seven steps:

a. Formatted the data into data tables including participant ID information and utterance sequence numbers.
b. Developed a theme codebook in tabular format to define linkages between numeric codes and theme categories. Logically organize the codebook based on your framework or report outline.
c. Determined face-sheet data categories on which retrieval will be done and add columns to the data tables to accommodate coding for these.
d. Did the thematic coding in the theme code column modifying the table as needed to handle text that should be coded with multiple themes.
e. Sorted the data by desired face-sheet data and theme code categories to look for patterns.
f. Validated the coding within a data table, correct and re-sort.
g. Merged appropriate data tables and validate coding across data tables. (Optional)

Step1: Format the interview data into tables

This step involves creating a four-column table, where each response of each speaker is entered. The key informant of focus group participant response rows would be interspersed with interviewer questions in separate rows.

Respondent Code	**Theme Code**	**Moderator question/ Participant Response**	**Sequence#**

Column 1: Contains the names of the speaker. For the purposes of anonymity, the respondents are identified by a unique ID instead of actual names.

Colum 2: This column will be used for categorical coding and indexing

Column 3: Contains the moderator question and the responses

Column 4: Chronological order of utterances at every speaker change.

After transcription, the themes can be identified and populated in column 2.

Step2: Developing a Theme Codebook

The responses were reviewed for the purpose of identifying the various themes that reoccur or that are significance for the study. This codebook contains a definition of each major theme and each sub-theme within a major theme. The codebook assigns numerical codes to the in vivo or constructed textual theme categories being defined. The theme codes will be used for the actual theme coding and numerical sort is done on theme codes in the data tables during analysis. The theme codes and sub-theme codes will be hierarchically assigned. The themes were be derived from the Saidah & Abdelbaki cloud governance model.

Table 5: Structure of Theme Codebook

Level			
1	**2**	**3**	**Theme**
1.0			Strategic trigger
	1.10		Business Process management
		1.11	Strategic alignment of cloud and business objectives
		1.12	Business case for cloud adoption

Source: Research

Step 3: Add Columns and Codes to Capture Face-sheet Data

After developing a theme codebook, the theme codes were populated in the table constructed in step 1.

Step 4: Coding Text Rows with One or with Multiple Theme Codes

Table 6: Theme coding and numbering

Respondent Code	Theme Code	Moderator question/ Participant Response	Sequence#
Moderator	1.11	**Cloud services alignment with overall business objectives**	24
A	1.111	There's no clear alignment of cloud and business objectives in my organization.	25
B	1.112	Yes, there's alignment of cloud and business objectives. Additionally, there's strong business case for cloud computing adoption	26

Source: Research

In this case, if the same response had more than one theme, an additional row was added and the themes split.

Table 7: Multi-theme response

Respondent Code	Theme Code	Moderator question/ Participant Response	Sequence#
Moderator	1.11	**Cloud services alignment with overall business objectives**	24
A	1.111	There's no clear alignment of cloud and business objectives in my organization.	25
B	1.111	Yes, there's alignment of cloud and business objectives.	26.01
B	1.112	Additionally, there's strong business case for cloud computing adoption	26.02

Source: Research

Step 5: Sorting Data Tables and Finding Patterns

Microsoft Word table sort function was used to sort data according to the different themes.

Steps 6 and 7: Code Validation/Correction and Merging of Data Tables

The research then read all text segments for each code and decided whether text segments are all instance of a particular category or if corrections are needed. Corrections were made to the table data will be resort.

ii. Quantitative Data Analysis

Quantitative data was collected by use of online-distributed questionnaire. Path analysis was used to establish the correlation between the research variables. Path analysis is considered one of the best ways to make causal inferences from correlation data (Freedman, 1987, 1997; Rogosa, 1987). The research used beta correlation to establish the causal correlation between the dependent variables and the dependent variable.

CHAPTER 4: RESULTS AND DISCUSSIONS

4.0 Introduction

This chapter presents an analysis of the findings on the cloud governance readiness of the organization under study. SPSS version 19.0 software was used to perform path analysis of the data collected through quantitative methods. Microsoft work was used for thematic content analysis of the Focus Group Discussion (FGD) data.

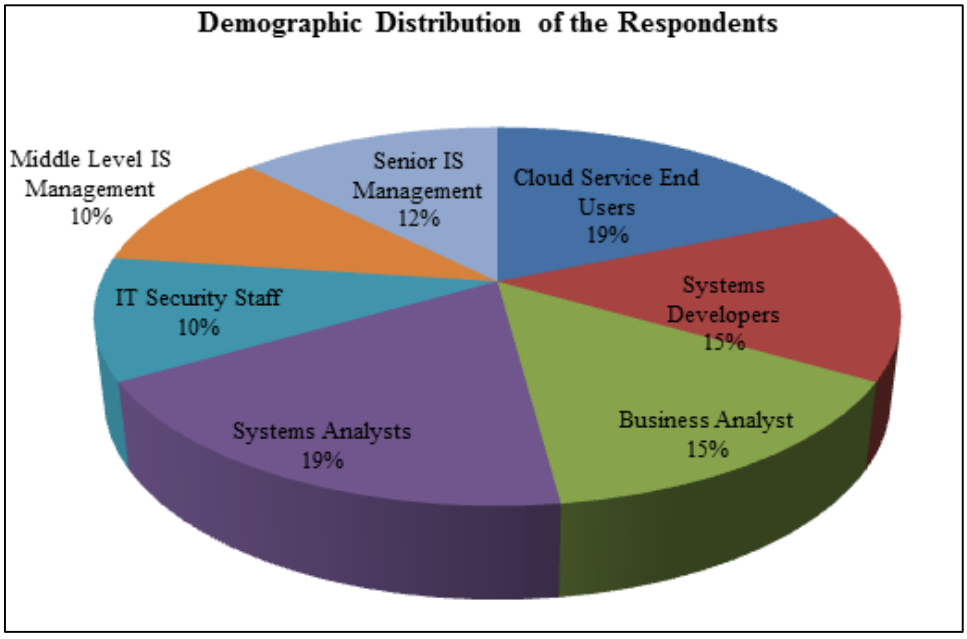
4.1 Response Rate

Out of the target population of 44 respondents, 30 respondents filled the online questionnaires and submitted back, while 5 respondents participated in Focus Group Discussion. This accounted for approximately 80% response.

4.2 Respondent demography

The focus of this study include senior IS management, Cloud Service end users, systems developers, business analysts, systems analysts, IT security staff and middle level IS management. The demographic distribution in terms of responses received is presented in the chart below:

Figure 6: Demographic distribution of the respondents



Source: Research

4.3 Thematic content Analysis of the independent variables

4.3.1 Analysis of responses for constructs measuring statements

The Likert scale in the questionnaire had five options, ranging from 1-5 ((1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree). During analysis, the first two (strongly disagree and disagree) were combined into disagree, and the last two combined into agree, resulting into three measures (agree, disagree and neutral).

i. Strategic alignment of cloud computing and business objectives

This research sought to establish whether there's a strategic alignment of cloud computing and the overall business objectives. From the responses, there's a clear strategic alignment of cloud computing objectives and the business objectives. 70% of the respondents indicated that there's a strategic alignment of cloud computing objectives with the overall business objectives, 16% disagreed while 14% were neutral. The research went further to analyze the demography of the respondents with regards to whether a strategic alignment exists. The responses were distributed as follows:-

Table 8: Distribution of responses on Strategic Alignment

Role in the organization	**Percentage (%)**
Cloud Service End Users	16
Systems Developers	11
Business Analyst	16
Systems Analysts	22
IT Security Staff	8
Middle Level IS Management	11
Senior IS Management	16

Source: Research

ii. Business case for cloud adoption

This research sought to establish the main reasons why the organization adopted or plans to adopt cloud computing services. 86% of the respondents indicated that by adopting cloud computing, they have or would achieve cross boundary trade and product market, improve employee productivity through value creation (91%), and gain competitive advantage (95%) through implementation of cloud-based Customer Relationship Management (CRM) and Social Relationship Management (SRM) systems. 93% indicated that implementing cloud services has enabled the organization contain the cost of IT operations, mainly by converting the IT Capital Expenses (CAPEX) to Operating Expenses (OPEX). Improving products or services had the least support (27%).

Table 9: Business Case for cloud computing

Reason for cloud adoption	**Percentage (%)**		
	Agree	**Neutral**	**Disagree**
Break Geographic Barriers	86	3	11
Develop products or services not possible without cloud computing	85	5	10
Contain Costs	93	0	7
Increase employee Productivity	91	9	0
Improve Products Or Services	27	67	6
Reach New Markets	68	27	5
Gain Competitive Advantage	95	5	0

Source: Research

The researcher further sought to establish to what extent cloud computing has achieved the objectives of its adoption in the organization by asking whether the cloud computing has helped the organization in achieving the overall business objectives. 100% of the respondents confirmed that cloud computing has enabled the organization to break the geographical barriers, 71% indicated that cloud computing has enabled the organization to develop products and services otherwise not possible without cloud computing, 64% confirmed that cloud computing has enabled the organization to contain IT costs, increased productivity (89%), improved existing products and services (35%), reached new markets (64%) and gained competitive advantage (89%). The results are summarized in table 10.

Table 10: Cloud computing contribution towards business objectives

Contribution towards Business objectives	**Percentage (%)**		
	Agree	**Neutral**	**Disagree**
Break Geographic Barriers	100	0	0
Develop products or services not possible without cloud computing	71	14	15
Contain Costs	64	20	16
Increase Productivity	89	10	1
Improve Products Or Services	35	17	48
Reach New Markets	64	24	12
Gain Competitive Advantage	89	11	0

Source: Research

iii. Cloud computing value measurement

The researcher sought to understand whether various mechanisms exist in the organization for measuring the value of cloud computing vs the risks involved to the organization. The measurement mechanisms identified include Annual Net Present Value (NPV) and Return on Investment (ROI) reports of cloud services, cost savings from hardware support, software license and hardware acquisition and cost reports compared with the budget allocation for cloud computing.

iv. Awareness of investments to be lost due to cloud adoption

The respondents were asked if the organization considered any investments that were lost or would be lost by adoption of cloud computing. The respondents identified these investments as some IT roles and processes and control over the sensitive data.

v. Resource Management

Under resource management, questions asked were about human resource and compute resources. The respondents were asked whether there's adequate skilled labor to support cloud computing in the organization. Though some respondents confirmed that there are skills to manage cloud services, most respondents indicated that skilled labor is still lacking or inadequate and the available resources require appropriate training to support the cloud services.

Concerning compute resource management, the respondents indicated that there is no clear policy to govern the provisioning of the virtual machines. Most respondents indicated that because of inadequate skills among the infrastructure team, only the administrator in charge of cloud services understands the process of provisioning virtual machines, and thus no control has been implemented.

vi. Data Access Management

As a data access management control, the respondents were asked if there exists an identity management strategy that governs access to cloud data. The respondents indicated that such strategies exist. They mentioned strategies like role-based user access, data governance policies, multi-factor authentication, and the IAM policies for both on-premise and cloud services. They further indicated that the cloud services in place fully support the identity management strategies. The internal processes fully support the identity management strategy according to the respondents. They cited internal processes like periodic auditing of the systems, monthly password reset policy, deletion of accounts of staff who have exited the company, reviewing of access logs, need-to-use access policy, and role-based access as some of the internal processes enforced to support the identity management strategy.

The respondents further indicated that there are mechanisms used by the CSP to allow the customers define the access to their data. They cited that the most used mechanism is security content automation protocol (SCAP), followed by logging mechanisms, IP address range controls, Active directory policies, server and database administrator access management, multi-factor authentication, access control list, and communication through ports on the need to use basis. The CSP also allows the customer to define the location and backup location of its data during the MV/storage service creation.

vii. Cloud Computing Risk Management

The respondents were asked whether both the business and IT are aware of the various risks that are associated with cloud computing and whether there are various risk mitigation measures to address these risks. The respondents indicated that both the business and IT are aware of the risks associated with cloud services and they have profiled these risks as unlimited access of the user data by the cloud providers, data storage location, cloud data and deletion, customers inability to access and manage the cloud infrastructures, and the limited rights to access and audit the security control. The respondents proposed the need for control to govern unprivileged user access, controls

to ensure that customer data is deleted when hardware is issue to another customer by CSP, and also right to enable customer to invoke electronic investigation procedures.

On cloud computing risk management, the respondents indicated that the enterprise risk management unit is responsible for formulating measures to be taken to control the risks associated with adoption of cloud services. They identified some of these controls as authorization and authentication strategy, digital signatures, encryption, time stamp logging, regular reviews of audit trails by security team and IAM policies to ensure data security.

Table 11: Summary of Risk Management Responses

Question	**Percentage (%)**		
	Agree	**Neutral**	**Disagree**
IT and the business are aware of the various risks associated with the cloud services in use in our organization	20%	47%	33%
There exist risk management measures to ensure the identified risks are reduced to acceptable levels	3%	80%	17%
Cloud computing risk management is part of Enterprise Risk Management	3%	93%	3%
The risk management controls are sufficient for our cloud services	60%	7%	33%

Source: Research

viii. Cloud Service Provider Code of Practice

As an important aspect of cloud computing governance, this research sought to establish if the respondents are aware of any code of practice publication by the CSP. The responses indicated that CSP has published complete cloud computing code of practice. The respondents indicated that this has published on the vendors' online website and the clients must understand its detailed terms and conditions, and sign it before acquiring the cloud service. The CSP also send hard copy to the client prior to contract signing. The clients are also informed of any changes in the policy appropriately.

ix. Cloud computing security management and auditing

Table 12: Security Management summary

Question	Percentage (%)		
	Disagree	**Agree**	**Neutral**
The Cloud Service Provider adheres to established security governance framework(s)	0%	73%	27%
The Cloud Service Provider undergo regular (e.g. annual) 3rd party audits for compliance with the established security governance frameworks	13%	17%	70%
The Cloud service provider allows clients to audit their data security controls	0%	77%	23%
The CSP has implemented multi-factor authentication for controlling access to cloud data	33%	27%	40%
The data security controls for our cloud services is sufficient	47%	37%	17%
There is assurance of data security and non-access from the CSP staff	0%	40%	60%
There is a clear security policy for cloud services in my organization	0%	50%	50%
The CSP provides end-to-end encryption for data in-transit	50%	27%	23%
The CSP offer encryption to its customers to use for data-at-rest	0%	47%	53%
The CSP uses formally vetted encryption algorithms (e.g., under NIST's FIPS 140-2) for securing customer data-at-rest	0%	50%	50%
There is a clear cryptographic key management responsibility for the cloud services	47%	53%	0%

Source: Research

a) User Account Audit

The respondents indicated that there is effective audit processes enforced periodically for better management of the user accounts. The audit process is carried out on the user account matrix, level of adherence to standard operations procedures, and disabling accounts of the staff who have exited the company. These audits also ensure that only authorized users are accessing given systems.

b) Authentication

The controls managing the risks associated with ubiquitous access have been identified according to the respondents. They cited control like: multi-factor authentication; access control list; data encryptions; role based access; digital signatures; time stamps and trail audits as some of the controls identified and enforced to avert cases of ubiquitous access. The cloud service too has met the need of these control requirements to a large extent, hence ensuring threats are averted. The respondents further alluded to the fact that these control have also offered a higher level assurance of authentication of the user of the cloud services systems.

c) Third Party Audits on CSP Platform

On whether the CSP terms and conditions allows for third party to audit the implemented and management of security control measures, the respondents indicated that there is a provision for this on a formal request as was stated in the contract scope and during the phase of vendor evaluation. Though it might have not been executed but there is a written agreement regarding it provision. According to the respondents, the CSP allows for performance of vulnerability scan and penetration testing of the service and its supporting infrastructure. These tests can be done by the organization itself or through the help of a third party on a schedule basis ranging from quarter-annually, semi-annually or annually. However, sometimes it is performed as a reactive measure in cases of threat alerts.

The respondents indicated that the CSP has been open in provision of its audited reports from their external auditor for scrutiny by third party vendor before the implementation on the cloud service and for periodic reviews. The request for this reviews are penned down in the contract agreement and once review is done, recommendations on new implementation and areas for improvement are followed up by the respondent's organization for appropriate close.

d) Client Reference Checks

On the part of CSP reference checks, the respondents agreed that the CSP provided them with contact details for their current customers. These according to them is a mandatory step is vendor selection process and a key component is the procurement process management of the I.C.T service providers. They said that reference checks forms the basis of benchmarking so that the organization does not fall short in their scope of implementation and selection of a reputable CSP.

e) Availability of published cloud computing code of practice

The CSP has published complete cloud computing code of practice. The respondents indicated that this has published on the vendors' online website and the clients must understand its detailed terms and conditions, and sign it before acquiring the cloud service. The CSP also send hard copy to the client prior to contract signing. The clients are also informed of any changes in the policy appropriately.

f) Data Encryption

On the part of data security, the respondent indicated that it's a shared responsibility between the organization and CSP to encrypt the data. The security of the data at rest relies squarely on the client since the CSP only provides the infrastructure, while data on transit is encrypted by the CSP. However, they indicated that in cases where the client cannot offer encryption to the data at rest, it can be done by the CSP using formally vetted encryption algorithms like AES-256 and IS 27001 and the encryption key is managed by CSP as well.

x. Audit Recommendation Implementation

The respondents indicated that the responsibility of implementing the audit recommendation is a shared responsibility between the cloud service provider and the organization. They indicated that issues of SaaS will be handled by the organization while those regarding IaaS are handled by the CSP. The timelines for execution of these recommendations are pegged on the existing SLA formulated during the signing of the contract.

xi. Service Level Management

The SLA is published on the management portal according to the respondents. The CSP always strive to meet and exceed the stated SLA targets to ensure they continuously delight their clients; this becomes advantage for them during reference checks. They also indicated that it's the sole responsibility of the IS Service Delivery manager to ensure that the SLA are met by analyzing the weekly systems availability report and the third party availability monitoring tool. The manager then compares these reports against the agreed SLA targets to conclude whether the SLA was met or violated. Most respondents rated CSP SLA performance as satisfactory.

The table below shows the summary of responses regarding Service Level Management:

Table 13: Service Level Management

Question	Percentage (%)		
	Disagree	Agree	Neutral
My organization has formulated and signed a measurable Service Level Agreement for cloud services	20	20	60
Incident management process for cloud services has been agreed on and is clear between my organization and the cloud service provider	100	73	17
Our Cloud Service Provider provides service availability monitoring and measuring tool	6.7	93.3	0
Change Management Process for the cloud services exists and it's clear to my organization	23.3	26.7	50
Problem and incident management processes for cloud computing is effective to my organization	53.3	36.7	10
I can rate the quality of cloud services we consume as excellent	3.3	30	66.7

Source: Research

a) Incident and configuration Management Processes

The roles of incident management, configuration management and service desk are vital in cloud service operation, management and governance as indicated by the respondents. They said that service desk gives them support all day support on cloud service incidents and requests, incident management helps in aligning incident resolution procedures, and configuration management helps in configuring user accounts and licenses.

b) Cloud Service Monitoring

The respondents were asked if there are various measurement mechanisms for the cloud services. They indicated that various mechanisms are used to measure the availability and SLA performance of the CSP. Some of the mechanisms identified include an on-premise monitoring tool that has the capability of monitoring the cloud services, availability monitoring tool on the cloud customer portal which has a dashboard with the various service availability reports, and the various CSP-generated reports which are obtained on request.

c) Cloud Service Change Management

On the existence of change management process, the respondent indicated that there exists a change management process in the organization. However, they said that it does not address well the cloud service change procedures and need serious modification. They said the modification of

this process should take an integrated approach involving both the organization and the CSP. The change process is the sole governance of the change management and there exist no exceptions to it.

xii. Backup and Recovery

Backup and recovery services are offered by the CSP for Software-as-a-Service (SaaS). For Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service, backup is the responsibility of the client. However, for PaaS and IaaS, backup and recovery services can be provided by the CSP as extra services.

On whether the CSP has mechanisms to ensure client data don't move to the geographical areas proscribed the client, the respondents indicated that the CSP is in-charge of both data at rest and data on transit in SaaS, and therefore it may not be easy to control or to have visibility into data movement. In PaaS and IaaS cases, the data location, backup and recovery locations are selectable by the client, thus it's easier to control data movement to ensure data doesn't reside in proscribed geographic location.

Table 14: Backup and disaster recovery summary

Question	**Percentage (%)**		
	Disagree	**Agree**	**Neutral**
The CSP allows customer to select specific location for use and/or storage of the customer data	20%	60%	20%
CSP provides technical enforcement to prevent a customer's data from moving through or to a customer proscribed location	20%	77%	3%
CSP allows a customer to select a separate, specific location for the back-up or replication of data that still meets any customer restrictions on the nation-state level of location restrictions	0%	13%	87%
The CSP offers data back-up and recovery services for customers	10%	67%	23%
The CSP allows customer to select specific location for use and/or storage of the customer data	57%	43%	0%

Source: Research

xiii. Exit Strategy

Responses indicate that the organization has clearly defined cloud exit policy. There also exist various measures to ensure that data is completely removed from the CSP servers. However, there is lack of assurance on the measures the CSP has in place to ensure that data is completely wiped of the cloud environment upon exit.

Table 15: Summary of Exit Strategy responses

Contribution towards Business objectives	**Percentage (%)**		
	Agree	**Neutral**	**Disagree**
My organization has a clear cloud exit policy	3%	73%	23%
The CSP adequately and satisfactorily handles data remanence issues to ensure proper and eventual removal of customer data upon exit	0%	80%	20%
There's a mature decommission process that involves Regulatory Standard-specified overwrite processes and independent verification of this process by an audit team	10%	43%	47%
SLA exists for data removal upon exit from cloud	0%	70%	30%
Exit policy is specified in the contract signed between the CSP and the client	0%	83%	17%
The customer can delete own data from cloud	60%	40%	0%
Third party audit is allowed to ensure complete removal of data upon exit	3%	63%	33%

Source: Research

Table 16: Summary of the findings based on Saidah & Abdelbaki Model

Model	**Sub-Model**	**Summary of the Result**
Policy	Data Policy	• There exists various data governance policies; both on-transit and at rest • Responsibilities on data security and well defined; both for the organization and the CSP
	Business Process Management Policy	• The organization has a clear business case for the cloud services • The organization has realized the benefits of cloud computing in terms of cutting operational IT costs, faster delivery of IT services as well as giving the organization a competitive advantage over the competitors.
	Exit Policy	• The organization has clearly defined cloud exit policy. There also exist various measures to ensure that data is completely removed from the CSP servers.
Operation	Authentication & Authorization	• Various identify management measures exist to ensure security of data in the cloud; however, the respondents are not confident that the measures adequately address security of their cloud data. • There are various internal processes and audit procedures that ensure proper management of identities and user accounts. • There are adequate control measures that govern ubiquitous access in the cloud. • The controls include multi-factor authentication
	Audit	• The CSPs allow third party audit on their cloud platforms • The CSPs share security third party audit reports on vulnerability tests with the client.

		• The responsibility of implementing audit recommendations depends on the cloud service; in case of IaaS and PaaS, it squarely rests with the client, in SaaS it's majorly the responsibility of the CSP. However, as noted from the responses, there should be a collaborative effort in ensuring successful implementation of the audit recommendations.
	Monitoring	• There are various cloud service monitoring tools; third-party tools and some provided by the CSP that helps the organization to manage the SLAs. • From the responses, most CSPs meet the SLAs
	Asset Management and Capacity planning	• Responses indicate that there are insufficient skills among the IT staff to handle cloud services. • There is no clear policy governing the provisioning of the compute resources.
Management	Security Management	• Data encryption is necessary for both data at rest and data in-transit. For SaaS services, encryption of data at rest is the responsibility of the CSP, while in cases of IaaS and PaaS; it's either the sole responsibility of the client, or a collaborative effort of both CSP and the client, depending on the contract. • For the CSPs that offer encryption solutions, these encryption algorithms are vetted under different encryption vetting programs. • IaaS and PaaS clients have the capability of selecting specific backup location, while in SaaS, backup location is at the discretion of the CSP.
	Service Management	• The organization has SLAs with the CSPs for all the cloud services • The respondents rated the CSP SLA performance as satisfactory • SLA monitoring tools exist; both provided by the CSP and third party tools

	Risk Management	• Both IT and the business are aware of the various risks associated with cloud computing • Various risk mitigation measures have been implemented to manage the cloud computing risks
	Change Management	• Even though a change management process exists in the organization, it doesn't adequately address cloud change activities, especially for SaaS services • Some exceptions exist for the change management process since the organization has no direct control on such changes.

Research: Research

4.4 Path Analysis

Path analysis was performed to determine the causal effect between the independent variables and the dependent variable. It was used to determine the effect of each of the independent variables identified in this research on cloud computing governance. The significance level (α) value for this research was 0.05, meaning any beta coefficient value (α) less than 0.05 was significant for the study, while a beta value more than this value was considered as not significant.

Table 17: Summary for Direct Predictors to the effective cloud governance

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.952[a]	.906	.870	.338	.906	25.187	8	21	.000

Predictors: (Constant), Security Management, ServiceMagament, Monitoring and Availability management, Risk Management, Capacity Management, Change Management, Exit Strategy, Expectation Management.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.019	.832		.022	.0982
	Availability management	.033	.392	.026	.084	.0934
	ServiceMagament	.092	.269	.092	.341	.0336
	Expectation Management	.777	.581	.686	1.337	.0196
	Capacity Management	.492	.446	.429	1.104	.0282
	Change Management	.460	.363	.564	1.265	.0220
	Exit Strategy	.419	.620	.341	.676	.0507
	Risk Management	.446	.336	.377	1.328	.0198
	Security Management	.581	.489	.533	1.188	.0248

Source: Research

a. Availability Management and Effective Cloud Governance

The table below shows the correlation between Availability Management and Effective Cloud Governance. Availability management has a both direct correlation with Effective cloud governance (β =0.26) as well as indirect correlation through Service Level Management (β=0.805), expectation management (β=0.6565), and capacity management (β= 0.399399). Availability Management is therefore an exogenous variable. The positive beta values between Availability Management and Effective cloud governance indicate that there is a direct positive correlation between the two variables. The indirect correlation between availability management and effective cloud governance will therefore be 1.1624, the sum of the products of all the paths **(0.875*0.092+0.957*0.686+0.931*0.429).** However, this path has an alpha value of 0.0934, which is greater than the significant value of 0.05; therefore this path is not significant.

i. Availability and Service Level Management Path Weight (β) = 0.875

A strong positive correlation of 0.875 exists between Service Level Management and Availability Management, with an alpha value of 0.000, which is less than the significant value of 0.05, thus this correlation is significant.

Table 18: Correlation between Availability and Service Level Management

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	-.129	.416		-.310	.759	-.980	.723
	Monitoring and Availability management	1.120	.117	.875	9.570	.000	.880	1.360

a. *Dependent Variable: ServiceMagament*

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.875[a]	.766	.757	.461	.766	91.579	1	28	.000

a. Predictors: (Constant), Monitoring and Availability management

Source: Research

ii. *Availability management and Expectation Management Path Weight (β) = 0.957*

Expectation Management has a strong positive correlation (0.957) with Availability Management. The alpha value for this path is 0.000, thus it is significant.

Table 19: Correlation between Availability management and Expectation Management

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.076	.219		.346	.732	-.373	.525
	Monitoring and Availability management	1.082	.062	.957	17.533	.000	.956	1.209

a. Dependent Variable: Expectation Management

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.957[a]	.917	.914	.243	.917	307.410	1	28	.000

a. Predictors: (Constant), Monitoring and Availability management

Source: Research

iii. *Availability management and Capacity Management Path Weight (β) = 0.931*

The capacity management has a strong positive correlation with availability management, and the alpha value is 0.000, which is lower than the significant value of 0.05, and therefore this correlation is significant to the study.

Table 20: Correlation between Availability management and Capacity Management

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
		B	Std. Error	Beta	T	Sig.	Lower Bound	Upper Bound
1	(Constant)	.011	.274		.038	.970	-.550	.571
	Monitoring and Availability management	1.039	.077	.931	13.480	.000	.881	1.196

a. Dependent Variable: Capacity Management

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.931[a]	.866	.862	.303	.866	181.718	1	28	.000

a. Predictors: (Constant), Monitoring and Availability management

Source: Research

b. Service Level Management and Effective Cloud Governance

There is a positive correlation between Service Level Management and Effective Cloud Governance (β= 0.092). This path has an alpha value of 0.0336 which is less than the significant level value of 0.05, thus this correlation is significant.

c. Expectation Management and Effective Cloud Governance

The beta correlation (β) between Expectation Management and Effective Cloud Governance is 0.686. This correlation is significant since it has an alpha value of 0.0196, which is less than the significant value of 0.05, thus this correlation is significant.

d. Capacity Management and Effective Cloud Governance

There is a beta (β) correlation of 0.429 between Capacity Management and Effective Cloud Governance. This is a positive correlation between capacity management and effective cloud

governance. Besides, this correlation is significant since it has an alpha value of 0.0282, which is less than the significant value of 0.05.

e. **Change Management and Effective Cloud Governance**

There is a strong correlation between change management and effective cloud computing governance ($\beta = 0.564$). This correlation is significant for the study of cloud governance readiness assessment in the organization since it has an alpha value of 0.0220, which is less than the significant value of 0.05.

f. Exit Strategy and Effective Cloud Governance

There is a positive correlation of 0.341 between exit strategy and effective cloud governance. The alpha value for this correlation is 0.0507, which is near to the significant value of 0.05, therefore this correlation is significant.

g. Risk Management and Effective Cloud Governance

Risk management positively correlates with effective cloud computing governance with a beta correlation of 0.377. The alpha value for this correlation is 0.0198, which is less than the significant value of 0.05, qualifying the correlation as significant for the study.

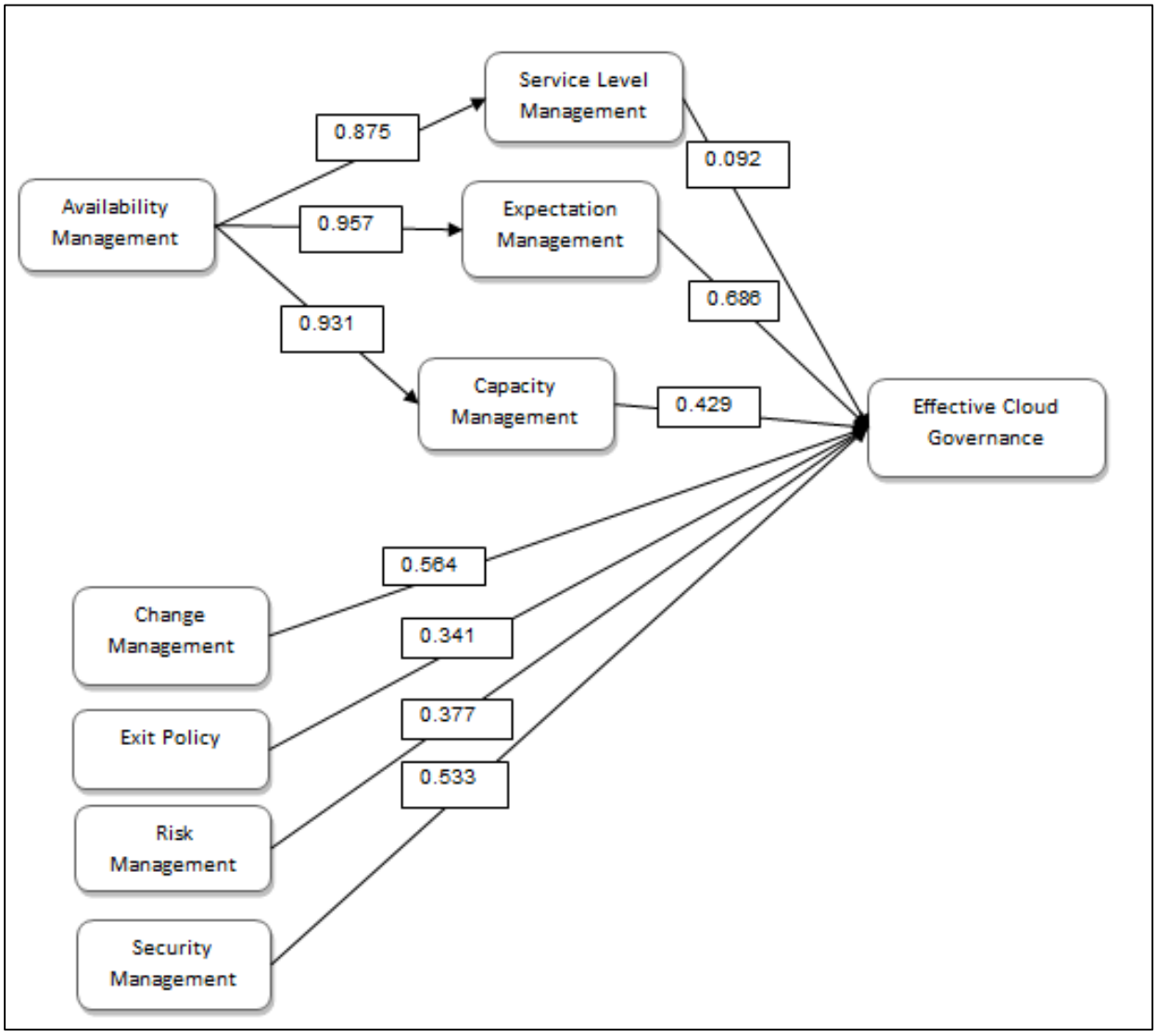
h. Security Management and Effective Cloud Governance

A beta correlation of 0.533 exists between Security Management and Effective Cloud Governance. This is a strong positive correlation which is significant to the study.

4.5 The conceptual model showing casual relationships and beta coefficient values

The figure 7 below shows the research conceptual model used in this research with the casual relationship between the variables and the corresponding *beta* coefficient values. The direct correlation between Availability management and the dependent variable has been excluded because the hypothesis is not supported.

Figure 7: Conceptual Model-Causal Relationship and Beta Coefficient values



Source: Research

4.6 The Governance Maturity Level of the Airline

The beta values of the variables were used as their weights or their effect on effective cloud computing governance. This research assumed that the perfect correlation between each of the independent variables and the dependent variable, and therefore this was used as the target beta value for each of the independent variables.

The table below shows the variable actual weights (beta values) against the target weight of 1, and gives the totals. Because there are a total of eight (8) independent variables, the total target weight is 8 (1*8).

Table 21: Variable target beta vs. actual beta values

VARIABLE	TARGET BETA VALUE	ACTUAL BETA VALUE
Monitoring and Availability management	1	0.026
ServiceMagament	1	0.092
Expectation Management	1	0.686
Capacity Management	1	0.429
Change Management	1	0.564
Exit Strategy	1	0.341
Risk Management	1	0.377
Security Management	1	0.533
Total	8	3.048

Source: Research

To assess the cloud governance maturity level, Cloud Governance Capability Maturity Model discussed in literature review was used. This research used **1.6** as the width of each level (between the minimum and the maximum limits). This was derived by dividing **8**, which is the total target by the number of levels **(5).** This was used to come up with the scale in the table below:

Table 22: Minimum and Maximum class widths for Cloud computing capability maturity levels

LEVEL	MINIMUM WEIGHT	MAXIMUM WEIGHT
Ad Hoc	0	1.6
Initial	1.6	3.2
Defined	3.2	4.8
Managed	4.8	6.4
Optimized	6.4	8.0

Source: Research

The organization, having a total beta value of 3.048 lies between 1.6 and 3.2, thus it's in the **initial** level of cloud governance maturity level.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter begins by evaluating the achievement of research objectives and outlines the recommendations. Finally, it highlights area that can be researched further.

5.1 Evaluation of Research Objectives

Objective 1: Identify the opportunities and challenges of cloud computing in the airline industry

In trying to achieve this research objective, respondents were asked the following question: *What are the major challenges in implementing cloud governance in the airline industry?*

From the research findings, several opportunities were identified in terms of the benefits offered by cloud computing. These were identified as:-

i. Sales increases since cloud services have helped the organization to break geographic barriers thus reach more clients.
ii. Hardware cost reduction since the client organization doesn't have to purchase hardware, but rather pay for these as a service offered by CSP
iii. Power consumption reductions since the servers are not hosted by the client organization.
iv. Reduced in total cost of ownership (TCO) on infrastructure because the organization doesn't acquire and maintain the hardware.
v. Cost of procuring and managing infrastructure has reduced as well as time to the market for acquiring computing resources.
vi. Server acquisition costs reduced from CAPEX to OPEX since no hardware is acquired.

The challenges of cloud computing were identified in terms of the risks involved in cloud computing. The challenges identified include:-

i. Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data
ii. Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information.
iii. Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud.

iv. The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.

v. Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

Objective 2: To determine the various factors that contribute to and the extent to which they influence effective cloud computing governance

In achieving this objective, the research validated the various hypotheses that were formulated. A path analysis was done to establish the correlation between each of the independent research variables and the dependent variable. Below is a summary of the hypotheses validation:

Table 23: Summary of Hypotheses validation

Hypothesis Code	Hypothesis statement	Result
H1	Existence of a Cloud computing Availability Management process has a direct positive impact on Effective Cloud Governance	Availability Management (AM) has a positive correlation with effective cloud governance. The correlation is even stronger through moderating factors (Service Level Management, Expectation Management and Capacity Management). The paths through these variables have alpha values of less than 0.05, thus are significant. However, the direct correlation between Availability management and effective cloud governance has an alpha value greater than 0.05, and therefore not significant for the study. This hypothesis is **not supported**
H2	Proper Service Level Management results into Effective Cloud Governance	Service Level Management (SLM) is an intervening variable between AM and the dependent variable (effective cloud governance). The correlation between SLM and the dependent variable is 0.092. This path has an alpha value of 0.0336, which is less than 0.05, thus this correlation is significant. This hypothesis is therefore **supported.**

H3	Existence of Expectation Management process for cloud services is significant for an Effective Cloud Governance.	There's a strong correlation between Expectation Management (EM) and the dependent variable. The alpha value of this correlation is 0.0196, which is less than 0.05 thus it's significant. This hypothesis is therefore **supported**.
H4	Cloud computing Capacity Management process is a recipe for an Effective Cloud Governance	Capacity Management (CAM) is an intervening variable between AM and the dependent variable. It also has a direct strong correlation with the dependent variable. This correlation has an alpha value of 0.0282, thus it's significant, and thus this hypothesis is **supported**.
H5	Effective cloud services Change Management policy enhances Effective Cloud Governance	Change management (CM) has a beta correlation of 0.564 with the dependent variable, which is a strong positive correlation. The alpha value for this correlation is 0.0220 which makes it significant. This hypothesis is therefore **supported**.
H6	A clear cloud Exit Strategy is for Effective Cloud Governance	The beta correlation between Exit Policy (EP) and the dependent variable is 0.341. The alpha value for this path is 0.0507, which is close to the significant value of 0.05, thus the hypothesis is **supported**.
H7	Risk Management policy for cloud services are important for Effective Cloud Governance.	Risk Management (RM) has a direct correlation with the dependent variable with a beta value of 0.377 5. The alpha value for thus correlation is 0.0198 which is less than the significant value of 0.05, thus the hypothesis is **supported**.

H8	Security Management policy is necessary for an Effective Cloud Governance	A beta correlation of 0.533 exists between Security Management (SM) and the dependent variable. The alpha value for this path is 0.0248, thus it is significant. This hypothesis is **supported**.

Objective 3: To develop a methodology to assess cloud governance readiness

A conceptual model in figure 5 was developed by identifying the various factors that contribute to effective cloud computing governance and how they are related to each other. Using this model, path analysis was performed on the various variables to get the degree of correlation between the independent and the dependent variables. The *beta* correlation coefficient values from path analysis were summed and compared with the class limits in table 22 to assess the cloud computing governance maturity level of the organization.

Objective 4: To use the developed methodology to assess the cloud computing governance readiness of a local airline company

The sum of all the beta correlation values was computed, and then compared with the class widths in table 11 to rank the cloud computing governance maturity level. In assigning the class widths, the assumption that the perfect correlation between each of the independent variables and the dependent variable is 1. The cloud computing governance in the organization was then ranked as being in the initial capability level.

5.2 Conclusion

To exploit the many benefits of cloud computing, an organization must develop a clear governance strategy and management plan. Cloud governance is critical to manage risk, adapt effectively, ensure continuity and helps in strategic alignment of cloud computing objectives with the business objectives. However, most organizations have not reviewed their IT governance practices to cover the new paradigms of computing like cloud computing. Besides, most of those that have cloud governance have no way of evaluating their cloud governance maturity. This research has presented a conceptual model and a methodology that an organization can adapt to assess their cloud governance readiness by determining their cloud governance maturity levels. We drew the following conclusions from the research findings:

i. Security controls implemented by the organization are not sufficient. Access to cloud services is majorly password-controlled. This exposes the company's data to external attacks.
ii. Even though data encryption has been implemented, there is no clarity on key management responsibility.
iii. There is no visibility of backup and restore locations for most of the cloud services. This may lead to the organization's data being backed up in regions proscribed by either the company policy or government legislation.

iv. The organization has no way of ensuring that all the data on cloud is deleted from the cloud service provider's disks upon exit.

v. There are inadequate skills among IT staff who manage cloud services.

5.3 Recommendations

i. Identity management

Even though respondents stated that there is multifactor authentication for some of the cloud services, this should be rolled out to the rest of services to ensure that there is adequate authentication and authentication of the users accessing cloud data.

ii. Data Encryption

The responses reveal that most of the CSPs implement data encryption as a data security measure. However, in some cases there is no clear definition of the responsibility of encryption key management. The organization and other cloud consumers should therefore ensure that this is defined in the contract so that there is accountability of key implementation. Moreover, the key management implementations majorly depend on the provider and therefore the need to carefully vet them to ensure they meet the tenant needs.

iii. Data Backup and recovery

From the research findings, there is lack of visibility of the data backup location especially for SaaS services. The organization should therefore insist on backup and recovery plan from the CSP, including the backup and recovery sites, in order to ensure that no data is stored in locations proscribed by the organization.

iv. Cloud Exit Policy

From the responses, it is clear that the organization has an exit policy for the cloud services. However, there is lack of clarity on CSP's method of handling data remanence or persistence on their cloud media. There should be more research in this area to come up with methodologies and practices to ensure that CSPs adhere to the data remanence and persistence standards.

Guarantees of complete data removal are unclear and not uniform among the cloud service providers. The industry should therefore identify and standardize the necessary regulatory measures to ensure complete data removal from the CSP media upon client exit.

v. Resource Management

Responses received confirm that skilled human resources in the area of cloud computing remains a major challenge for the organization in an attempt to exploit the various opportunities offered by

cloud computing. The organization should therefore identify and address the knowledge gap with regards to cloud computing by empowering the staff through training.

Additionally, there should be a clear process of provisioning cloud virtual machines as well as user accounts to ensure cloud resources are efficiently used.

5.4 Limitations and recommendations for further work

This research is not without limitations. First, it is a case study in just one organization, therefore may not be the true picture of the airline industry or general cloud computing usage in Kenya. Secondly, it focused on all the service models as well as all the deployment models. The findings would be different if a specific service model or deployment model was focused. Finally, the researcher made the assumption that the perfect correlation between independent and the dependent variable is one, and therefore used it as the target beta correlation for each of the variables, since no other suitable method was available in the literature reviewed. We therefore recommend further research in this area, which has not been widely researched compared to other aspects of cloud computing.

REFERENCES

Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114.

Alvarez, Vanessa, James Staten and Jessica McKee. Assess Your Cloud Maturity. Cambridge: Forrester Research, 2012.

Axelos (2014) IT service management and cloud computing

https://www.axelos.com/CMSPages/GetFile.aspx?guid=ede50958-eccb-46e1-b982-7816100d8fb9

Retrieved on May 10th, 2016.

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

Bibi, S. Katsaros, D. & Bozanis, P., 2012. Business Application Acquisition: On-Premise or SaaS Based.

Bisong, A. and Rahman, S.S.M. (2011).An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45.

Blaisdell Rick (2015) "How cloud computing could help the aviation industry" https://www.rickscloud.com/how-cloud-computing-could-help-the-aviation-industry/

Choundhary, V. (2007). Software as a service: Implications for investment in software development. Proceedings of 40th Hawaii International Conference on System Sciences - 2007.

Cisco (2010). Managing the Real Cost of On-Demand Enterprise Cloud Services with Chargeback Models.

Cloud Security Alliance (CSA, 2010) http://www.cloudsecurityalliance.org/

Cloud Security Standards: What to Expect & What to Negotiate. http://www.cloud-council.org/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf

Retrieved on May 10th, 2016.

Dimension Data (2013) Cloud Readiness Consulting Services http://www.dimensiondata.com/Global/Downloadable%20Documents/Cloud%20Readiness%20Consulting%20Services%20Brochure.pdf

Dukaric, R. and Juric, M.B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210.

Gartner (2013).Gartner IT Glossary - Cloud Computing. Retrieved Friday, May 29, 2015, from http://www.gartner.com/it-glossary/cloud-computing/

Gartner, 2012. Forecast: Software as a Service, All Regions, 2010-2015, 1H12 Update.

Grance, T., & Mell, P. (2011, September).The NIST Definition of Cloud Computing.

Guo, Z., Song, M., & Song, J. (2010). A Governance Model for Cloud Computing. Paper presented at the Management and Service Science (MASS).

He, Y (2011) The Lifecycle Process Model for Cloud Governance. University of Twente.

ISO, International Organization for Standardization (2005a). ISO/IEC 20000- 1:2005 IT Service Management - Specification. ISO, Switzerland. 1st edition. 16 pages.

Jadhwani, Prem. Cloud Computing Building a Framework for Successful Transition. White Paper. Herndon: UNICOM Government, 2009.

KPMG."Exploring the Cloud: A Global Study of Government's Adoption of Cloud." 2012.

Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 28, 833–851.

Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58.

LaPelle, Nancy R. (2004) Simplifying Qualitative Data Analysis Using General Purpose Software Tools; University of Massachusetts Medical School.

Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.

Mattoon, Scott , Bob Hensle and James Baty. Cloud Computing Maturity Model - Guiding Success with Cloud Capabilities.White Paper. Redwood Shores: Oracle, 2011.

Mell, P. and Grance, T. "The NIST Definition of Cloud Computing," Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, Sep. 2011.

Microsoft.(2010). Cloud Governance.from http://azuredecisions.com/2010/06/10/cloud-governance/

Mircea, M. (2012).Addressing Data Security in the Cloud. World Academy of Science, Engineeringand Technology, 66, 539-546.

Mourad, Mohamed and Hussain, Mohammed (2014) "The Impact of Cloud Computing on ITIL Service Strategy Processes" International Journal of Computer and Communication Engineering, Vol. 3, No. 5, September 2014. http://ijcce.org/papers/351-C024.pdf Retrieved on May 10th, 2016.

NIST Special Publication 800-145: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Ogigau-Neamtiu, F. (2012).Cloud Computing Security Issues. Journal of Defense Resource Management, 3(2), 141-148.

Omwansa, T. , Waema, T. and Omwenga, B. (2014) Cloud Computing in Kenya: A 2013 Baseline Survey

University of Nairobi School of Computing and Informatics (SCI) & Computing for Development Lab (C4DLab)

Ramesh, R.K et al (2014) "Nth Third Party Auditing For Data Integrity In Cloud", Asia Pacific Journal of Research, Vol: I Issue XIII,

Rasheed, Hassan (2003) "Auditing for Standards compliance in the cloud: challenges and directions" The International Arab Journal of Information Technology, Vol. 1, No. 0, July 2003

Richardson, David (2010) "Ready Your Infrastructure for the Cloud", Emerson Network Power http://www.techdata.ca/(S(lbgqlvv4htbr43yf14mvqv55))/avocent/files/Emerson_Network_Power_Cloud_WP_0511.pdf

Ristola, Jaakko (2010) Information Technology Service Management for Cloud computing

http://lib.tkk.fi/Dipl/2010/urn100243.pdf Retrieved on May 10th, 2016.

Saidah, Ahmed, and Abdelbaki, "A New Cloud Computing Governance Framework," CLOSER 2014, 4th International Conference on Cloud Computing and Services Science, April 3–5, 2014, Barcelona, Spain. Sen, Jaydip (2012) Security and Privacy Issues in Cloud Computing, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India.

Schmidt, P. and Grabski, V (2014) "Proposing a Cloud Computing Capability Maturity Model,"Proceedings of the 6th Annual SIG-ASYS Conference, December 2014, Auckland, NZ.

Shaker Saidah, Ahmed, and Nashwa Abdelbaki, "A New Cloud Computing Governance Framework,"

Sentinel research (2014) "Cloud Readiness Assessment: Adopting Cloud to your business strategy"
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.scc.com%2Fwp-content%2Fuploads%2F2014%2F09%2FSCC-Sentinel-Cloud-Readiness-Assessment.pdf&ei=_DxbVcqPJon-UoH0gCg&usg=AFQjCNGHf2hsCSItIKwCxGtguP1yjDP97A&sig2=vPhxyniLZ88OhuuaSq-x9w&bvm=bv.93564037,d.d24

Thomas, B., Ullrich, T(2011): Cloud-Readiness – Continental IT Corporate Infrastructure & Security Strategy (based on cloud readiness at continental AG Presentation developed by Krings, K., Dalbert, U., Workshop 'eco-verband der deutschen Internetwirtschaft e.v.', Cologne, Germany)

Trivedi, H. (2013) Cloud Adoption Model for Governments and Large Enterprises. Massachusetts Institute of Technology, Cambridge.

Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16, 102-107.

APPENDICES

Appendix 1: Questionnaire

Dear Respondent,

This questionnaire is intended to gather research data as part of an academic investigation for my Master of Science in Information Technology Management at the University of Nairobi.

The information obtained will not be used for any other purpose other than to enhance the body of knowledge in the Academic Research area computing governance. I kindly request you to take your time to complete the questionnaire to the best of your knowledge and thereafter send the same back to me.

Your participation is highly appreciated.

Thank you.

Stephen O. Owuonda

---

1. What is your role in the organization regarding cloud computing?

Cloud Service End Users	
Systems Developers	
System Developers	
Business Analyst	
Systems Analysts	
IT Security Staff	
Middle Level IS Management	
Senior IS Management	

2. What are the main reasons why your organization has adopted/ intends to adopt cloud computing? (1=Least Reason, 5=Main Reason)

	Break Geographic Barriers	**1**	**2**	**3**	**4**	**5**
	Develop products or services not possible without cloud computing					
	Contain Costs					
	Increase Productivity					
	Improve Products Or Services					
	Reach New Markets					
	Gain Competitive Advantage					

3. Cloud Service and deployment models

a) What cloud service models have you implemented in your organization?

Software-as-a-Service	
Infrastructure-as-a-Service	
Platform-as-a-Service	

b) Cloud Deployment Models

Public Cloud	
Private Cloud	
Community Cloud	
Hybrid Cloud	

4. Awareness and involvement in cloud governance among the employees (1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

		1	2	3	4	5
i.	I can accurately describe cloud governance in my organization					
ii.	I'm personally involved in formulation of cloud computing policies, standards and procedures in my organization					
iii.	Cloud Governance in my organization is based on a cloud governance model					

5. Business Case for cloud computing (1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

		1	2	3	4	5
i.	Business goals and cloud computing objectives are aligned					
ii.	Cloud computing services have helped in achieving the overall business objectives					
iii.	We're able to develop important cloud computing policies that apply throughout the institution					
iv.	We agree on measurable goals for cloud services with the cloud service provider(s)					
v.	We incorporate measurement and reporting in our Cloud computing governance process					
vi.	The organization has adequate asset management policy for cloud services					
How influential is cloud governance in your organization in producing the following outcomes (1=Not influential, 5=very influential)						
vii.	Cost-effective use of IT resources					
viii.	Effective use of IT to enhance achievement of business objectives					
ix.	Business process re-engineering					

6. Risk Management(1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

i.		**1**	**2**	**3**	**4**	**5**
ii.	IT and the business are aware of the various risks associated with the cloud services in use in our organization					
iii.	There exist risk management measures to ensure the identified risks are reduced to acceptable levels					
iv.	Cloud computing risk management is part of Enterprise Risk Management					
v.	The risk management controls are sufficient for our cloud services					

7. Service Management (1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

		1	2	3	4	5
i.	My organization has formulated and signed a measurable Service Level Agreement for cloud services					
ii.	Incident management process for cloud services has been agreed on and is clear between my organization and the cloud service provider					
iii.	Our Cloud Service Provider provides service availability monitoring and measuring tool					
iv.	Cloud Service Provider continually improves cloud services offered to the clients					
v.	Change Management Process for the cloud services exists and it's clear to my organization					
vi.	Change management process was formulated collaboratively by my organization and the CSP					
vii.	Problem and incident management processes for cloud computing is effective to my organization					
viii.	I can rate the quality of cloud services we consume as excellent					

8. Security Management (1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

		1	2	3	4	5
i.	The Cloud Service Provider adheres to established security governance framework(s)					
ii.	The Cloud Service Provider undergo regular (e.g. annual) 3rd party audits for compliance with the established security governance frameworks					
iii.	The Cloud service provider allows clients to audit their data security controls					
iv.	The CSP has implemented multi-factor authentication for controlling access to cloud data					
v.	The data security controls for our cloud services is sufficient					
vi.	There is assurance of data security and non-access from the CSP staff					
vii.	There is a clear security policy for cloud services in my organization					
viii.	The CSP provides end-to-end encryption for data in-transit					
ix.	The CSP offer encryption to its customers to use for data-at-rest					
x.	The CSP uses formally vetted encryption algorithms (e.g., under NIST's FIPS 140-2) for securing customer data-at-rest					
xi.	There is a clear cryptographic key management responsibility for the cloud services					

9. Data Location ,Data Backup and Recovery Schemes for Recover and Restoration (1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

		1	2	3	4	5
i.	The CSP allows customer to select specific location for use and/or storage of the customer data					
ii.	CSP provides technical enforcement to prevent a customer's data from moving through or to a customer proscribed location					
ii.	CSP allows a customer to select a separate, specific location for the back-up or replication of data that still meets any customer restrictions on the nation-state level of location restrictions					
v.	The CSP offers data back-up and recovery services for customers					

10. Exit strategy (1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)

		1	2	3	4	5
i.	My organization has a clear cloud exit policy					
ii.	The CSP adequately and satisfactorily handles data remanence issues to ensure proper and eventual removal of customer data upon exit					
ii.	There's a mature decommission process that involves Regulatory Standard- specified overwrite processes and independent verification of this process by an audit team					
v.	SLA exists for data removal upon exit from cloud					
v.	Exit policy is specified in the contract signed between the CSP and the client					
vi.	The customer can delete own data from cloud					
ii.	Third party audit is allowed to ensure complete removal of data upon exit					

Appendix 2: Focus Group Discussion Guide

1. **Cloud Authentication & Authorization Policy Management**
   a. Does your organization have an identity management strategy?
   b. If yes, does the cloud service support your organization's identity management strategy?
   c. Is there an effective internal process that ensures that identities for cloud services are managed throughout their lifecycle?
   d. Is there an effective audit process that is actioned at regular intervals to ensure that user accounts are appropriately managed?
   e. Have the controls required to manage the risks associated with the ubiquitous access provided by the cloud been identified?
   f. If yes, what controls are these?
   g. Does the cloud service meet those control requirements?
   h. Is there a higher level of assurance required that the party using an identity is the authorized user of the account when authenticating to the service? (I.e. is multi-factor authentication necessary?)
   i. Does the service provider's Terms of Service allow the agency to directly audit the implementation and management of the security measures that are in place to protect the service and the data held within it?
   j. Does the cloud service meet those control requirements?
   k. If yes, does this include performing vulnerability scans and penetration testing of the service and the supporting infrastructure?
   l. Will the service provider allow the agency to thoroughly review recent audit reports before signing up for service? (E.g. will the service provider provide the Statement of Applicability together with a copy of the full audit reports from their external auditor, and the results of any recent internal audits?)
   m. Will the service provider enable potential customers to perform reference checks by providing the contact details of two or more of its current customers?
   n. Has the service provider published a completed Cloud Computing Code of Practice?
   o. Who is responsible for the implementation of the audit recommendations?
2. **Cloud Service Management**
   a. Is there a clear Service Level Agreement (SLA) between your organization and the cloud service provider?
   b. Who in your organization is responsible for ensuring the SLAs are met?
   c. How are the SLAs monitored?
   d. In a scale of 1-5 (1=Poor,2=Bad, 3=Fair, 4=Good, 5=Excellent), how do you rate the service provider in terms of meeting the SLAs?
   e. Is there a cloud service change management process in your organization?
   f. If Cloud Service Change Management process exists, do you think it is appropriate for the services used by your organization?
   g. Are there exceptions to this process, i.e. situations when this process is bypassed? (Explain)
   h. Incident management, configuration management and service desk is important for our cloud services

3. **Security Management**
   a. What mechanisms does the CSP provide for customers to define access to their data?
   b. Does your CSP provide any technical enforcement to prevent a customer's data from moving through or to a customer proscribed location?
   c. Does your CSP allow a customer to select a separate, specific location for the back-up or replication of data that still meets any customer restrictions on the nation-state level of location restrictions?
4. **Encryption and Key Management Practices**
   a. Does your CSP provide end-to-end encryption for data in-transit?
   b. Does the CSP offer encryption to its customers to use for data-at-rest?
   c. If your CSP does offer encryption to its customers to use for data-at-rest, then does the CSP use formally vetted encryption algorithms (e.g., under NIST's FIPS 140-2)?
   d. If the CSP uses formally vetted encryption algorithms, under what specific program(s) have these encryption algorithms been vetted?
   e. If the CSP does offer encryption to its customers to use for data-at-rest, then how is (cryptographic) key management handled (i.e., by the CSP or by the customer?)
   f. Does your CSP offer data back-up and recovery services for customers?
5. **Cloud services alignment with overall business objectives**
   a. Business goals and cloud computing objectives are aligned
   b. Cloud computing services have helped in achieving the overall business objectives
   c. IT and the business are aware of the various risks associated with the cloud services in use in our organization
   d. If yes, what are these risks?
   e. Do measures exist to ensure the identified risks are reduced to acceptable levels?
   f. If risk management measures exist, what specific measures has your organization implemented?
   g. Has the management formulated strategies to measure and track the value of cloud return vs. risk?
   h. Has the management considered what existing investments might be lost in their cloud planning?
   i. Does the Cloud Service Provider (CSP) adhere to any established governance framework(s) involving data security controls?
   j. If yes, which framework(s) does your CSP follow?
   k. If yes, does the CSP undergo any regular (e.g. annual) 3rd party audit(s) for compliance with any established governance framework(s)?
   l. Does the CSP allow customers to audit the CSP's data security controls?
   m. What mechanisms does the CSP provide for customers to define access to their data?
   n. Does your CSP provide any technical enforcement to prevent a customer's data from moving through or to a customer proscribed location?
6. **Exit Strategy**
   a. Does your organization have a clear policy on the exit strategy?
   b. How does your CSP handle the issue of data remanence or persistence and which method(s) does a CSP utilize to ensure that removed data is indeed removed?
   c. What guarantees does a CSP provide for the timeliness of the removal of data?
7. **Does your organization involve all the stakeholders in the cloud governance activities?**

Appendix 3: Theme Codebook

Level			
1	**2**	**3**	**Theme**
1			Strategic trigger
	1.1		Business Process management
		1.11	Strategic alignment of cloud and business objectives
		1.12	Business case for cloud adoption
		1.13	Contribution of cloud computing towards business objectives
		1.14	Cloud computing value measurement
		1.15	Awareness of investments to be lost due to cloud adoption
	1.2		Service Discovery
	1.3		Capacity Planning
		1.31	Human Resource Capacity
		1.32	Computing resource capacity planning (VMs, user accounts)
		1.33	Budget allocation for cloud services
	1.4		Exit strategy
		1.41	Exit policy availability
		1.42	Data Remanence
	1.5		Reference checks
2			Define and align
	2.1		Data policy
		2.11	Data movement policy
		2.12	Data Access policy
		2.13	Organizational support for data policy
		2.14	Lack of organizational support for data policy
		2.15	Effectiveness of data policy
		2.16	Data Encryption
	2.2		Policy Management
	2.3		Integration
		2.31	Integration with on-premise systems

		2.32	Integration with other cloud systems
	2.4		Risk management
		2.41	Risk awareness by both IT and the business
		2.42	Existence of risk mitigation measures
		2.43	Suitability of the risk mitigation measures
	2.5		Service policy
	2.6		CSP code of practice
3			Build and implement
	3.1		Authentication
		3.11	User account audit
		3.12	Multi-factor authentication
		3.13	Password strength
	3.2		Authorization
	3.3		Asset management
	3.4		Configuration management
	3.5		Roles and responsibility
4			Deliver and measure
	4.1		Service delivery
	4.2		Service Level Management
		4.21	Existence of SLAs
		4.22	SLA Measurement
		4.23	CSP SLA performance
		4.24	SLA responsibility matrix
	4.3		Auditing and logging
		4.31	Third party audit
		4.32	Audit recommendation implementation responsibility
		4.33	Audit report review by the client
	4.4		Expectation management
5			Operation and feedback
	5.1		Monitoring

	5.2		Adaptation & transformation
	5.3		Service improvement
	5.4		Change management
		5.41	Existence of change management process
		5.42	Suitability of Change Management process
		5.43	Exceptions to Change Management process
	5.5		General effectiveness of the processes
	5.6		Backup and recovery
		5.61	Backup and recovery responsibility
		5.62	Backup and recovery location
6			Stakeholder involvement

Focus Group Discussion (FGD) Results

Category	Question	Response	Remarks
Cloud Service Governance Operation			
Cloud Authentication & Authorization Policy Management	Does your organization have an identity management strategy?	• Giving role-based access to cloud services • Strict data governance policies • Implementation of multi-factor authentication • Integration of users' IAM components into standardization processes	The responses indicate that most of the respondents are aware of the existence of identity management strategy exists in the organization. **Yes: 95%** **No: No%**
	If yes, does the cloud service support your organization's identity management strategy?	• To some extent • Full supported • Not sure • Identity management doesn't adequately address the challenges of cloud computing.	From the responses, most respondents are not confident that the IM strategies adequately support their cloud services. **To some extent: 35%** **Full supported: 40%** **Not supported: 25%**
	Is there an effective internal process that ensures that identities for cloud services are managed throughout their lifecycle?	• Yes, quarterly audit of the user matrix for the cloud services • Monthly password resets • Access and identity management strategy	These two questions seem to be overlapping in terms of responses received. However, the responses indicate that there exist internal processes and audit procedures to ensure proper management of identities and audits of user accounts.
	Is there an effective audit process that is actioned at regular intervals to ensure that user accounts are appropriately managed?	• Yes, quarterly audit of the user matrix for the cloud services • Monthly password resets • Yearly IS audit • Periodic review of access logs	

	Have the controls required to manage the risks associated with the ubiquitous access provided by the cloud been identified?	• Yes	Respondents asserted that various controls exist for ubiquitous access of cloud services. **Yes: 100%** **No: 0%**
	If yes, what controls are these?	• Role-based access • Personal identifiable information • Hashes • Digital Signatures • Time-stamps • Audit trails	Respondents clearly identified the various controls in place.
	Does the cloud service meet those control requirements?	• Yes; to some extent • To a larger extent; yes	All the respondents agreed that the CSPs meet the control requirements.
	Is there a higher level of assurance required that the party using an identity is the authorized user of the account when authenticating to the service? (I.e. is multi-factor authentication necessary?)	• Multi-factor authentication has been implemented in addition to password authentication. • Use of private/public keys • Password complexity/ strength policy must apply for all the passwords.	The respondents confirmed that in addition to password authentication, there are other authentication factors to ensure data security. **Yes: 100%** **No: 0%**
	Does the service provider's Terms of Service allow the agency to directly audit the implementation and management of the security measures that are in place to protect the service and the data held within it?	• This was in the contract but has never been executed. • Not sure if they allow audit on the implementation and management of the security measures	From the responses, it's clear that the organization is not keen on ensuring the security measures are implemented and effectively managed. **Yes: 30%** **No: 45%** **Not sure: 25%**
	Does the cloud service meet those control requirements?	• Yes; the controls in the cloud services used in the company are sufficient	Majority of the respondents admitted that the cloud services meet the requirements.

		• Yes; even though not excellent, the controls are adequate • To some extent	**Yes: 95%** **No: 5%**
	If yes, does this include performing vulnerability scans and penetration testing of the service and the supporting infrastructure?	• Yes; vulnerability scans and penetration tests are performed yearly on the cloud service/ infrastructure. • Vulnerability scans done when there is a security alert • Vulnerability scans can be done on demand, from either the organization or the CSP. • Not sure.	Most respondents asserted that the CSP shares third party reports on vulnerability test results. Additionally, most of the confirmed that their CSPs are compliant to one or more security frameworks. **Yes: 97%** **No/Not sure:3%**
	Will the service provider allow the agency to thoroughly review recent audit reports before signing up for service? (E.g. will the service provider provide the Statement of Applicability together with a copy of the full audit reports from their external auditor, and the results of any recent internal audits?)	• Yes- this was a requirement during CSP evaluation according to most respondents. • This is mandatory; yearly the organization ensures that the annual CSP report is obtained for review • Not sure if this happens; the respondents are not in a position to tell because they belong to operations rather than policy/ administration sections.	Most users admitted that the most recent audit reports are open for scrutiny by the cloud clients. **Yes: 90%** **No/Not sure: 10%**
	Will the service provider enable potential customers to perform reference checks by providing the contact details of two or more of its current customers?	• Yes- was a requirement during CSP evaluation according to most of the respondents • Since the other clients are known, especially for the CRM cloud service, reference checks in terms of benchmarking is always done	Most clients asserted that the CSP provide relevant reference checks. **Yes:100%** **No: 0%**
	Has the service provider published a completed Cloud Computing Code of Practice?	• Yes-Published on the management portal	In all cases, the respondents admitted that the CSP has a published code of practice.

		• Yes- Published on the portal and one is prompted to accept before creating any service. • Before adoption, the CSP ensures that the client fully understands the terms of use as well as code of practice.	**Yes: 100%**
	Who is responsible for the implementation of the audit recommendations?	• The cloud service provider is fully responsible(SaaS cloud service users) • The client is responsible for implementation of audit recommendations (IaaS user) • Both CSP and the client	The responsibility for implementation of audit reports varies, depending on the service model. For SaaS, most of implementation tasks are performed by the vendor (CSP) while in IaaS and PaaS it rests with the client in most cases.
Cloud Service Management	Is there a clear Service Level Agreement (SLA) between your organization and the cloud service provider?	Yes- The SLA is published in the portal • Yes- the SLA is agreed during contract agreement • SLAs are published on the management portal • The organization and the CSP further reviewed the existing SLAs.	All responses confirmed existence of SLAs. **Yes: 100%**
	Who in your organization is responsible for ensuring the SLAs are met?	• IT Manager • Service Delivery Manager • IT Project Manager • The application owner	Responsibility for implementation of SLAs varies depending on the organization structure of the respondents.
	How are the SLAs monitored?	• System monitoring tool • Cloud Service Portal has a monitoring tool • There are dashboard reports on the portal to monitor system activity	The various monitoring tools varied with the cloud service used. However, all the respondents admitted that SLAs are monitored in one way or another.

		• The system availability time reports provided by CSP on request • Third-party monitoring tool which has the capability of monitoring service availability. • Monitoring as a service; the vendor has a monitoring tool that can be used as a service.	
	In a scale of 1-5 (1=Poor,2=Bad, 3=Fair, 4=Good, 5=Excellent), how do you rate the service provider in terms of meeting the SLAs?	• 3; at times the CSP carries out planned maintenance during peak business hours without informing the clients • 5; the CSP has ensured maximum availability of the service • 4; response time in case of an incident is good. • 5; the CSP informs the organization well in advance in terms of a planned downtime.	Generally, the respondents rated CSP SLA performance as good or excellent. **Excellent: 30%** **Good: 50%** **Fair: 20%**
Security Management	What mechanisms does the CSP provide for customers to define access to their data?	• Security Content Automation Protocol (SCAP) control implementation through a third party cloud security vendor • Logging mechanisms • IP ranges controls • Timestamps. • Access Control Lists • Access control systems relating to active directory policies, servers, database, and administrator access management.	All the respondents indicated that there are various mechanisms provided by CSP to define access to their data. Some of these measures were used by many clients, while some were specific to given organizations.

	Does your CSP provide any technical enforcement to prevent a customer's data from moving through or to a customer proscribed location?	• The customer defines their preferred data location among the locations available to the vendor • The customer selects their preferred location from the portal.	Respondents especially those using IaaS and PaaS have the ability to define data location. Most SaaS consumers are however not very conscious about the location of data.
	Does your CSP allow a customer to select a separate, specific location for the back-up or replication of data that still meets any customer restrictions on the nation-state level of location restrictions?	• Yes- the customer selects among the available locations • The CSP has the freedom of choice; backup and recovery is the responsibility of the CSP	Like the previous question, IaaS and PaaS consumers can choose the backup location; however, SaaS clients are in most cases not concerned with the backup location.
Encryption and Key Management Practices	Does your CSP provide end-to-end encryption for data in-transit?	• No- data in transit is under the jurisdiction of the customer • CSP provides encryption of data in-transit. • Yes – the CSP assists in moving data from on-premise to the cloud. This involves encrypting the data • Though data in-transit is under the control of the client, the CSP can assist when called upon.	Generally, the respondents admitted that the CSP provides/ can provide encryption to data in-transit. **Yes: 75%** **No: 25%**
	Does the CSP offer encryption to its customers to use for data-at-rest?	• Yes; security of data at rest is the responsibility of the CSP since they are in charge of the database and backups • Encryption is offered at an extra cost • Security of data at rest is the responsibility of the client since the CSP only provides the platform	**Yes: 87%** **No: 13%**
	If your CSP does offer encryption to its customers to use for data-at-	• Yes; the organization requested for the vetting report from the CSP	**Yes: 60%** **No/Not Sure: 40%**

	rest, then does the CSP use formally vetted encryption algorithms (e.g., under NIST's FIPS 140-2)?	• Though never verified, the CSP indicated the vetting body of their encryption algorithm	
	If the CSP uses formally vetted encryption algorithms, under what specific program(s) have these encryption algorithms been vetted?	• Advanced Encryption Standard (AES)-256 • ISO 27001 • Not sure of the algorithm	Even though most users confirmed that the CSP uses formally vetted algorithms in the last question, most of them could not however identify these specific programs under which the algorithms are vetted. Only 25% of the respondents could identify these programs, while the remaining 75% couldn't identify the programs.
	If the CSP does offer encryption to its customers to use for data-at-rest, then how is (cryptographic) key management handled (i.e., by the CSP or by the customer?)	• Customer has the full responsibility • Both on client-side (Private Key) and server-side (CSP-Public key).	In most responses, the client has the full responsibility of key management (77%). 15% of the respondents indicated that there is a joint effort in ensuring the encryption keys are implemented.
	Does your CSP offer data back-up and recovery services for customers?	• Can be created as an extra service at the client's cost • Yes; the CSP ensures backup exists for the cloud service. • Backup is the responsibility of the client • The CSP offers high availability solutions to the clients; these are implemented at a cost.	Backup and recovery services are offered by the CSP depending on the kind of service consumed. For SaaS clients, the CSP offers backup and recovery services. However, for IaaS and PaaS clients, backup and recovery is the full responsibility of the client.

Change Management	Is there a cloud service change management process in your organization?	• Yes; it's addressed by the IS change management policy which adequately covers it • The change management process available doesn't adequately address the change requirements of cloud services.	Even though a change management process exists in the organization, there is no change management process that is specific to cloud services. IaaS and PaaS changes are adequately covered by the change management process since the organization has the full responsibility, however, for SaaS users, there is the general view that the organization may not be in control of the changes, and therefore the change management process isn't very effective.
	If Cloud Service Change Management process exists, do you think it is appropriate for the services used by your organization?	• Yes – all the changes are adequately tracked • No; most of the changes are done by the CSP and are mandatory, so the change management policy in place doesn't help.	
	Are there exceptions to this process, i.e. situations when this process is bypassed? (Explain)	• Yes; the changes done on the CSP side are not guided by this policy • For the changes that are done by the CSP, there is no control from the client side, and therefore are exceptions. • For changes on the IaaS and PaaS services, the organization has some control on the changes, for example moving from one VM to another, therefore they are not exempted from the change process, however, SaaS changes are carried out by the CSP, and therefore they may be exceptions.	65% of the responses indicated that there are no exceptions to change management process; these were majorly from the IaaS and PaaS consumers. However, 35% of the respondents, who are mainly SaaS users indicated that the changes are carried out by the CSP and therefore not under direct control of the client.
	Incident management, configuration management and	• Yes; ensures resolution of requests and incidents within the SLAs by	Generally, the respondents agreed that incident management, configuration

	service desk is important for our cloud services	channeling the requests to the appropriate people. • Incident management by third party has proved to be more effective than for on-premise services.	management and service desk are important in ensuring availability as well adequate support for the cloud services.
Cloud Service Governance Policy Management			
Cloud services alignment with overall business objectives	Business goals and cloud computing objectives are aligned	• Yes; the business needs drove the organization to adopt cloud computing • There was a clear business case for the cloud service; the business believed that it would offer a competitive advantage • No clear alignment	93% of the respondents understood the strategic alignment of business and cloud computing objectives. 7% of the respondents couldn't however confirm that there was a business case and alignment.
Business Case for cloud computing	Cloud computing services have helped in achieving the overall business objectives	• Yes; it's helped in converting IT CAPEX to OPEX • Cost containment has been achieved; this is a key business objective. • It has provided a competitive advantage to the organization	From the responses 94% confirmed that these services have helped the organization in achieving its overall objectives. 6% of the respondents however indicated that these services haven't helped the organization in achieving the overall business objectives.
	IT and the business are aware of the various risks associated with the cloud services in use in our organization	• Yes; risk analysis of the cloud incorporated both IT and the business. • These risks are only known to IT • Though the business initially didn't understand these risks, IT has helped the organization to identify and understand them, as well as the possible mitigation measures.	Generally, the responses indicated that both the business and IT are aware of these risks.

	If yes, what are these risks?	The various risks identified by the respondents include:- • Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data • Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information. • Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud. • The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations. • Customers cannot easily assure the security of systems that they do not	Most respondents were able to identify the risks as well as the various mitigation measures.

		directly control without using SLAs and having the right to audit security controls within their agreements.	
	Do measures exist to ensure the identified risks are reduced to acceptable levels?	• Yes- the organization has identified and implemented some measures to manage the risks • The organization has identified the risks; some of them being managed while some have been accepted.	
	If risk management measures exist, what specific measures has your organization implemented?	• Authentication & authorization • Digital signatures • Audit trails • Encryption	
	Cost-effective use of IT resources	• Up/ down-scaling on a need basis therefore provisioning resources as required • Few IT staff needed to support/ maintain IT services since most tasks are performed by the CSP. • No overhead costs such as data center cooling costs, hardware support as well as software licensing costs.	The respondents generally admitted that cloud services have helped the organization in ensuring effective use of IT resources, as well as effective use of IT to enhance achievement of business objectives.
	Effective use of IT to enhance achievement of business objectives	• Reduced turn-around time in provisioning of resources • Reduced time in delivering new business requirements • Increased availability of the applications	
	Has the management formulated strategies to measure and track the value of cloud return vs. risk?	• Yes; the cost reports are compared against the budget for the cloud services. • SLA reports	All the respondents agreed that the organization has formulated strategies to measure and track

		• Cost savings from hardware support, software license and hardware acquisition. • Controlled provisioning of virtual machines • Controlled account creation/ use of licenses	the value of cloud return vs risks involved. **Yes: 100%**
	Has the management considered what existing investments might be lost in their cloud planning?	• Yes; the respondents acknowledged that some of the roles/ functions will be lost with the adoption of cloud computing.	**Yes: 100%**
	Does the Cloud Service Provider (CSP) adhere to any established governance framework(s) involving data security controls?	• Yes • Not sure • Not aware of any	Most respondents were not aware of the cloud governance frameworks. However, a few had an idea of framework used by the CSP. **Yes: 3%** **No/Not sure: 97%**
	If yes, which framework(s) does your CSP follow?	• The CSP has got its own governance framework; Microsoft Cloud Governance Model	
	If yes, does the CSP undergo any regular (e.g. annual) 3rd party audit(s) for compliance with any established governance framework(s)?	• Not regular, but happens on demand • Done during annual IS audit • It happens, but no certainty of the frequency.	Most respondents are not sure/ aware of any framework.
	Does the CSP allow customers to audit the CSP's data security controls?	• Yes, the organization performs annual IS audits, including third-party platforms.	All the respondents were in agreement that the CSP allows security audits on their platforms.
	What mechanisms does the CSP provide for customers to define access to their data?	• Third-party encryption algorithms • Audit trails • Role-based access provision • Access control list for the servers • Use of private/public key authentication	All the respondents were aware of the various mechanisms provided by the CSP to define data access.

		• Use of multi-factor authentication	
	Does your CSP provide any technical enforcement to prevent a customer's data from moving through or to a customer proscribed location?	• The data location is visible and controlled by the client, not by CSP • The client must consent before data is moved to a different location.	Most respondents confirmed that the CSP provides mechanisms to prevent data from moving to proscribed locations. **Yes: 93%** **No/Not sure: 7%**
Exit Strategy	Does your organization have a clear policy on the exit strategy?	• Yes; this is clearly defined • The contract between the organization and the CSP clearly defined the exit process and the responsibility of either party • Not very clear for some services.	From the results, the organization has clear exit strategy for most of the cloud services. **Yes: 96%** **No: 40%**
	How does your CSP handle the issue of data remanence or persistence and which method(s) does a CSP utilize to ensure that removed data is indeed removed?	• Third-party auditing • Physical destruction of the media storing the data • The SLA states that the data should be completely wiped from the CSP premises. However, issues of remanence are not clear. • The CSP enables the client to delete the VMs thus wiping all the data.	The respondents were able to identify the various ways in which the CSP handles data remanence.
	What guarantees does a CSP provide for the timeliness of the removal of data?	• Exit strategy clearly defines the removal process and the guarantees • Service-level agreements (SLAs) • Master Service agreements with the customer • Contract guarantees • Services organization archive and mark data for deletion upon customer request.	Most respondents cited the various ways in which the CSP guarantees that data will be removed within the agreed time.