International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.8, April 2016 – www.ijais.org

Cloud Computing Governance Readiness Assessment: Case Study of a local Airline Company

Stephen O. Owuonda
University of Nairobi
P.O Box 791-00100, Nairobi.

Dan Orwa, PhD
University of Nairobi
P.O Box 30197-00100, Nairobi.

ABSTRACT
Cloud computing has attracted interest from both and public sector, especially the organizations that seek innovative ways to save money while increasing the trust and value of their IT systems. It 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. Despite these advantages it offers against on-premise IT platforms; many enterprise customers are still reluctant to deploy their business in the cloud. Additionally, many organizations that have adopted cloud services did so without clear cloud governance policies; therefore they fail to reap the many benefits that cloud computing offers. Further, most organizations don't have mechanisms to measure their cloud governance maturity, and therefore may not identify the opportunities of improvement in their cloud governance for better value delivery. This research sought to assess the cloud governance readiness of a local airline by identifying the various opportunities cloud computing offers as well as the challenges it presents to the organization, establish the various factors that contribute to and the extent to which they influence effective cloud governance in the organization, determine the cloud computing capability maturity level of the organization's and give recommendations on how the organization can improve cloud governance to attain a higher maturity level.

General Terms
Cloud computing governance

Keywords
Cloud Governance, security, public cloud, private cloud, hybrid cloud, cloud computing capability Maturity Model

1. INTRODUCTION
Cloud computing is a new paradigm shift in computing that has been adopted by organizations seeking innovative ways to save money and increase the trust and value of their information systems. As noted by Trivedi (2013), many organizations, both public and private sector are either moving to cloud or thinking about cloud. 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".

Agile path, a renowned IT research company observed that every new piece of technology creates a vacuum in the form of key IT disciplines that will help with the adoption, insertion and value creation from that new technology. This is true in the case of cloud computing; it offers a challenge in acquisition processes, as it differs with the traditional IT acquisition processes. As with other emerging information technology trends, various many existing IT management and governance policies are strained with the adoption of cloud governance. Organizations have the challenge of extending IT policies, standards and governance practices to cloud services.

From the wider industry perspective, the industry standards tend to lag behind for early adopters of these new technologies such as cloud computing as proven methodologies and guidelines are always missing for such technologies.

Agile Path (2013) further noted that cloud governance issues become more critical, particularly from security, risk, interoperability, portability and vendor lock-in perspectives. To navigate these challenges and deliver value from cloud computing investments, an organization needs a clear cloud computing governance framework, which should be continually reviewed to address emerging challenges. 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).

For an organization to review its cloud governance framework, it is necessary to have a mechanism of identifying the opportunities of improvement in the existing governance framework. This research presents a model that an organization can use to evaluate its cloud governance practices and rate itself in terms of cloud governance maturity. By using this model, an organization can identify the opportunities of improvement so as to attain a higher maturity level.

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.

H2: Proper Service Level Management results into Effective Cloud Governance
H3: Existence of Expectation Management process for cloud services is significant for an Effective Cloud Governance
H4: Cloud computing Capacity Management process is a recipe for an Effective Cloud Governance
H5: Effective cloud services Change Management policy enhances Effective Cloud Governance

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

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

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

2. RELATED WORK

2.1 Cloud Computing Definition

As a new paradigm in Information Technology, cloud computing has attracted enormous interest both in research and practice (Loebbecke and Ullrich, 2011). Cloud computing has been defines 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 is a delivery of all those 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) on the other hand defines cloud computing as nothing more than a service model where business workloads are deployed, transparently executed internally or somewhere on the internet, and businesses only pay for what they consume.

Another definition of cloud computing is by Gartner, which defines it as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies. Cloud computing is an emerging IT development, deployment and delivery model, enabling real time delivery of products, services and solutions over the internet (IDC)

Huthmacher (2010) quotes Green (2009)] to have observed that even through several experts have tried to define cloud computing, most agree that cloud computing contains a common change of computer processing, storage, hardware, software delivery, interfaces, business processes and also personal collaboration.

Based on the scope and objectives of this study, this study adopts the NIST definition of cloud computing.

2.2 Characteristics of Cloud Computing Models

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

a) On-demand self-service:- unilateral provisioning of computing capabilities (i.e. server time and network storage) is performed automatically, without human interaction with a service provider.

b) Broad network access: - Capabilities are available over the network via thin or thick client platforms, such as mobile phones, tablets, laptops, and workstations.

c) Resource pooling- Multiple consumers are served using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

d) Rapid elasticity: - The provider can elastically (sometimes automatically) provision and release resources commensurate with demand. To the consumer, the capabilities often appear to be unlimited and can be appropriated in any quantity at any time.

e) 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).

2.3 Cloud services Delivery Models

1. **Infrastructure as a Service (IaaS):** Service provision model which entails provisioning of fundamental computer resources (e.g., processing, storage, networks) (NIST, 2010). Ramesh et al. (2014) describe this as a model where cloud service provider supplies the resources on demand basis from their data centers. Giovanoli (2011) observes that "IaaS is similar to SaaS to the extent that a product is offered through the internet to a client as an on-demand service".

2. **Platform as a Service (Paas)**, which entails provision to users of the capability to deploy onto the cloud infrastructure applications created by the user with provider-supported programming languages and tools. The Cloud Service provider supplies the resources on demand basis from their Data centers (Ramesh et al., 2014). Giovanoli (2011) defines PaaS as a paradigm for delivering operating systems and associated services over the internet without downloads or installation. Giovanoli further adds that operating system features can be changed and upgraded frequently in PaaS model.

3. **Software as a Service (SaaS)**, which entails 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". He adds that the cloud user needs to pay to use the cloud software applications. Salesforge (2009) on the other hand describes SaaS as a way of delivering applications over the internet as a service. Salesforge further adds that instead of installing and maintaining software, through Service Oriented Architecture (SOA) approaches an organization can simply access it via the internet. Security Management, availability, and performance of a SaaS application is vendor-Managed

(Salesforge, 2009). Choundhary (2007) estimated SaaS growth to be 50% per year.

2.4 Cloud implementation models

1) **Private Cloud:** This infrastructure is owned by a single organization. Ramesh et al. (2014) states that it is a model where cloud infrastructure is owned by a private organization and they maintain their own auditing principles and process. They further add that private clouds don't connect to other clouds on the internet; therefore there are lesser chances of external attacks. Giovanoli (2011) states that private deployment model is suitable for large enterprises with an existing IT infrastructure.

2) **Public Cloud:** Open for public and is available in public networks (Ramesh et. al, 2014). A public cloud can connect to other public clouds, and the limitation on the number of users who can connect to public cloud depends on the service provider's capacity. There is less transparency of Service Level Agreement (SLA) between the service provider and the cloud user; therefore there are higher chances of violation (Ramesh et al. 2014). Giovanoli (2011) observed that public model is the mainstream model with the widest distribution and publicity, where IT infrastructure is hosted, operated and managed in one or more data centers by a third-party vendor. Giovanoli (2011) stated that public clouds offer dynamic, fine-grained, self-provisioned services via internet with web applications and web services to clients. He further states that these services are usually highly standardized parts of business processes.

3) **Community cloud:** belongs to several organizations, they will share among this type of infrastructure. They will manage internally or by a third party (Ramesh et. al, 2011).

4) **Hybrid cloud:** Combination of two or more Private, Public and Community clouds. Huthmacher (2010) states that hybrid cloud offers the possibility to put the applications with important security or legal concerns in a private cloud and other less significant applications can be hosted by a cloud provider. Huthmacher however states that the big challenge is the integrated implementation of a traditional IT environment with the public and/ or private cloud.

2.5 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). It involves establishing chains 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.

IT governance is part of corporate governance that pertains to it processes and supports the goal of business (2011). COBIT (2005) defines IT governance as decision rights, accountability framework and processes to encourage desirable behavior in the use of IT. This research adopts this definition of cloud governance by COBIT. 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.

IT governance has four deliverables; 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. As observed by Bailey & Becker (2014), extending governance to the cloud complicates IT governance.

Mangiuc (2001) on the other hand 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 that despite the numerous benefits cloud offers, there should be proper considerations regarding 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 before an organization moves to cloud. Bailey & Becker suggested that to mitigate the potential risks of extending governance to the cloud paradigm, organizations should put in place and sustain a practical governance framework to ensure cloud infrastructure and operations are as secure as traditional IT governance approaches.

One of the major aspects of cloud governance, which is security management, remains a major challenge for cloud service users. 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, various researchers have suggested the adoption of cloud governance (Guo, Song & Song, 2010; O'Neill, 2009).

He (2011) states that there is need to have a formal cloud governance structure to support transition to cloud computing. He further explains that the governance structure can establish an approach for the organizations to reduce risks, maintain business alignment, and maximize the value of cloud computing through a combination of people, process, and technology.

Many researchers argue that Service Oriented Architecture (SOA) governance can be leveraged for cloud settings (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 and managed appropriately and that services are able to develop in line with 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 local

divisions or departments issues to prioritize usage based on 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 (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 right behavior of services.

2.6 Cloud Governance Models

2.6.1 Microsoft's Cloud Governance Model

This model was developed for Microsoft Azure cloud platform, and it mainly focuses on policy management (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). He (2011) states that these three components work together to ensure correct versioning, scale and ensure security compliance.

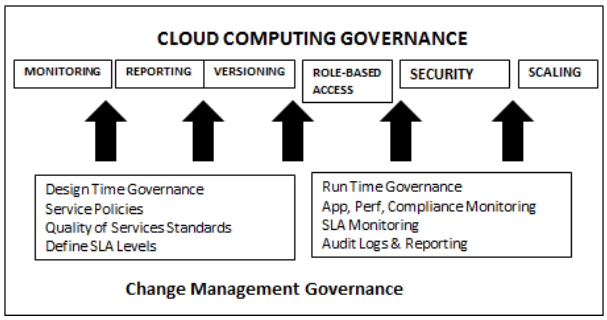

Figure 1: Microsoft's Cloud Governance Model

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.

2.6.2 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.

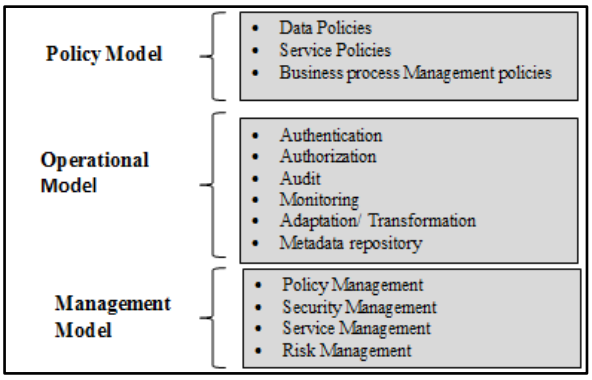

Figure 2: Cloud Governance Model from Guo et al.

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.

2.6.3 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.

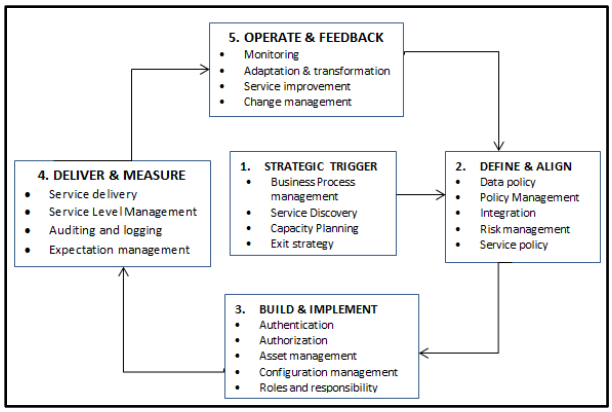

Figure 3: Saidah & Abdelbaki Cloud Governance Model

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 ensures that cloud services are aligned to the business needs and actively supports them. 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 is a mandatory process if an infrastructure already exists. It defines the integration between the cloud service and an existing infrastructure.

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 will use this model since it comprehensively covers all the dependent and independent variables that are key to this study.

2.7 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.

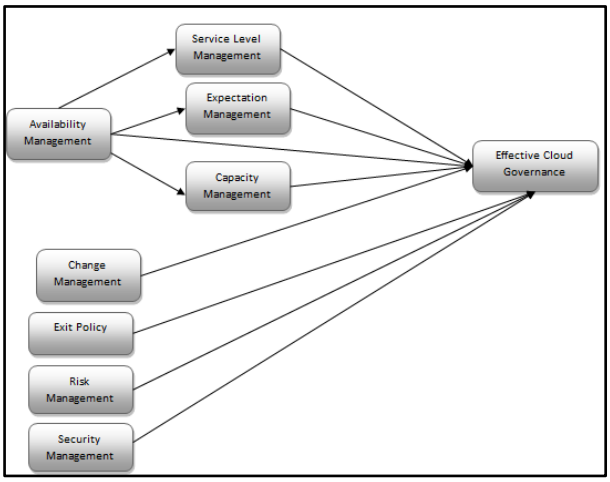

Figure 4: Conceptual Model

3. RESULTS AND DISCUSSION

3.1 Results

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.

Below is a summary of the predictors of effective cloud computing governance:

Table 1: Summary of the variable beta co-efficient

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	.0736
	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

Dependent Variable: Has Cloud Governance has been enhanced by the process

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.

Availability and Service Level Management

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 signification.

Table 2: Availability and Service Level Management

Coefficients[a]

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

Availability management and Expectation Management

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 3: Availability management and Expectation Management

Coefficients[a]

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

Availability management and Capacity Management

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 4: Availability management and Capacity Management

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			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

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			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

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) 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.

f) 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.

g) 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.

h) Change Management and Effective Cloud Governance

There is a strong correlation between change management and effective cloud computing governance (β = 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.

3.2 The conceptual model showing casual relationships and beta coefficient values

The figure below shows the research conceptual model used in this research with the casual relationship between the variables and the corresponding beta coefficient values.

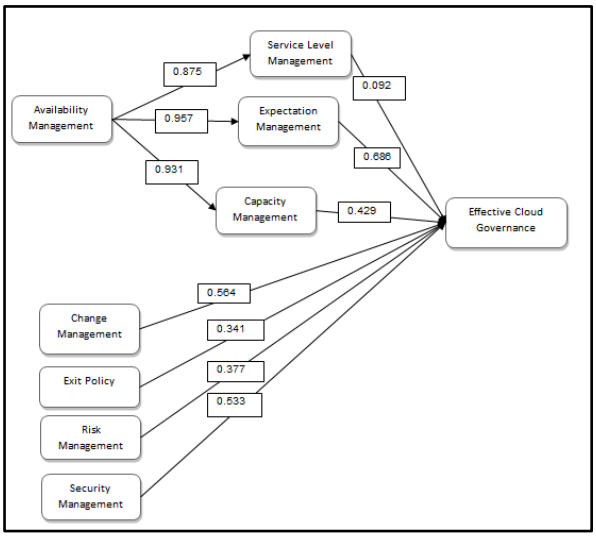

Figure 5: Conceptual Model-Causal Relationship and Beta Coefficient values

3.3 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 5: Variable target beta vs actual beta values

VARIABLE	TARGET BETA	BETA
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

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 6: 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

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.

4. CONCLUSIONS AND RECOMMENDATIONS

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, the research 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:-

- Sales increases since cloud services have helped the organization to break geographic barriers thus reach more clients.
- Hardware cost reduction since the client organization doesn't have to purchase hardware, but rather pay for these as a service offered by CSP
- Power consumption reductions since the servers are not hosted by the client organization.
- Reduced in total cost of ownership (TCO) on infrastructure because the organization doesn't acquire and maintain the hardware.
- Cost of procuring and managing infrastructure has reduced as well as time to the market for acquiring computing resources.
- 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:-

- 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 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 7: Summary of Hypotheses validation

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**.
H8	Risk Management policy for cloud services are	Risk Management (RM) has a direct correlation with the dependent variable with a beta

	important for Effective Cloud Governance.	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**.

Objective 3: To determine the cloud computing capability maturity level of the organization's cloud governance.
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.

Objective 4: Give recommendations on how the organization can improve its cloud governance policy in order to achieve a higher maturity capability level.

1. *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.

2. *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.

3. *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.

4. *Cloud Exit Policy*
   From the responses, it's 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.

5. *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. 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 governance of cloud services. 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.

6. REFERENCES

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

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

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

[4] Dimension Data (2012) Cloud "Readiness Consulting Services"http://www.dimensiondata.com/Global/Downloadable%20Documents/Cloud%20Readiness%20Consulting%20Services%20Brochure.pdf

[5] 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.

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

[7] Charles, G (2008) IT Governance-Leveraging ITIL V2/V3 for Governance Success. CA Incorporation.

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

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

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

[11] Dimension Data (2013) Cloud Readiness Consulting Serviceshttp://www.dimensiondata.com/Global/Downloa

dable%20Documents/Cloud%20Readiness%20Consulting%20Services%20Brochure.pdf

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

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

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

[15] Grance, T., & Mell, P. (2011, September). *The NIST Definition of Cloud Computing.* Retrieved May 28, 2015, from National Institute of Standards and Technology -

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

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

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

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

[20] Khazanchi, D. and Munkvold, B. E. 2000. Is information systems a science? An inquiry into the nature of the information systems discipline. *The data BASE for Advances in Information Systems 13*, 24 - 42.

[21] 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.

[22] KPMG (2012) "Assessing the Audit Impact of Cloud Computing"

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

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

[25] 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.

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

[27] Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.

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

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

[30] 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)

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

[32] Richardson, D. (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

[33] 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.*

[34] 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.

[35] 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

[36] The European Network and Information Security Agency (ENISA), "Cloud Computing:

[37] 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)

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

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