Journal of Information Technology & Software Engineering

OPEN ACCESS Freely available online

Research Article

Cloud Computing Governance Readiness Assessment: Profiling

Jeremiah Osida Onunga*

Department of Renewable Energy & Technology, Turkana University College, Lodwar, Kenya

ABSTRACT

Cloud computing makes the dream of computing real as a tool and in the form of service. This internet-based ongoing technology which has brought flexibility, capacity and power of processing has realized service-oriented idea and has created a new ecosystem in the computing world with its great power and benefits. Cloud computing is revolutionizing the Information Technology (IT) industry by enabling organizations to have flexible costs by buying a service instead of owning their assets. This will enable Universities to transfer their processing and storage to cloud for easy access by students. Nevertheless, decision makers in IT organizations have difficulties in evaluating Cloud services because there are no guidelines or any structured form to decide what Cloud services they should use. Cloud computing has emerged as an important platform to seeking innovative ways to save money and increase the trust and value of their information systems. 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 assessed cloud computing readiness of Turkana University College, Kenya by identifying the various opportunities cloud computing offers as well as the challenges it presents to the University. Path analysis was used to establish the various factors that contribute to and the extent to which they influence effective cloud governance in the University College. In this paper, author proposed a model based on a set of criteria to evaluate Cloud services that consists in six groups of thirty measurement criteria. In order to evaluate this proposal to make demonstrations with Google Apps and Microsoft Office 365. Author made interviews with clients, suppliers, and experts of Cloud services. Author also presented different major factors in cloud computing performance and analyzed and evaluated cloud performance in various scenarios considering these factors. The results of path analysis and the set criteria model were used to determine the cloud computing capability maturity level of the University College.

Keywords: Cloud services; Information Technology; Google Apps; Microsoft Office 365; Capital Expenses

INTRODUCTION

Cloud computing has emerged as an important platform to organizations and institutions of higher learning seeking innovative ways to save money and increase the trust and value of their information systems. Organizations across business, academics and public sector spectrum 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".

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

Correspondence to: Jeremiah Osida Onunga, Department of Renewable Energy & Technology, Turkana University College, Lodwar, Kenya, Tel no: 254724124661; E-mail: jerryosida@gmail.com

Received: October 19, 2021, **Accepted:** November 02, 2021, **Published:** November 09, 2021

Citation: Onunga JO (2021) Cloud Computing Governance Readiness Assessment: Profiling. J Inform Tech Softw Eng. 11: 271.

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 noted that more than 75% of the annual IT budget is spent on the cost for operating and managing the applications. However, author 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 therefore suggest that application rationalization is one of the ways to disentangle this issue. They state that adopting cloud services is a potential option towards cost saving initiatives, especially when rationalized applications are moved to the cloud. Gartner 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 [1].

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.

MATERIALS AND METHODS

Cloud computing

As a new paradigm in Information Technology, cloud computing has attracted great interest both in higher education research and practice. 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 (eg. 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, cloud computing involves delivery of IT services throughout a network such as the internet [2]. 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.

In conclusion, many researchers and institutions have tried to define cloud computing in different ways; however, as observed by many and 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.

Characteristics of cloud computing models

Dallas Chapter of Institute of Internal Auditors identified the following characteristics of cloud computing

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.

Broad network access: There is anywhere and anytime access to the cloud services *via* internet through thin or thick client platforms, such as mobile phones, tablets, laptops, and workstations.

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.

Rapid elasticity: The compute resources can be automatically scaled in and out, up and down commensurate with demand.

Measured service: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [3].

Cloud services delivery models

Infrastructure as a Service (IaaS): This is a service model where provisioning of compute resources (eg., processing, storage, networks) is done over the internet.

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.

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. give an alternative name to SaaS as "On-Demand Software Services (ODSS)". Security Management, availability, and performance of a SaaS application is vendor-managed. Choundhary estimated SaaS growth to be 50% per year [4,5].

Cloud implementation models

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 [5].

Public cloud: This is a cloud deployment model where the services are available on public networks and is open for public access [5].

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 [6].

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 [6].

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. 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.

Cloud governance

Cloud governance is part of IT governance, which is a subset of corporate governance. Saidah and Abdelbaki 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 [7].

As part of corporate governance, IT governance that pertains to IT processes and supports the goal of business in an organization [6]. He, 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 [6].

Deliverables of IT governance includes business growth, cost effectiveness, asset utilization, and business agility. Author 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.

Cloud governance models

Microsoft's cloud governance model: Microsoft cloud governance model's major focus is policy management and was developed for Windows Azure cloud platform. 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, stated, these three components are work in an integrated manner to ensure correct versioning, scale an ensure security compliance [6].

Guo's cloud governance model: This model has been identified by various researchers as the first proposed academic model for cloud governance [6,8]. It discusses the aspects of cloud governance in general [6]. 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.

Saidah and Abdelbaki model: Saidah and Abdelbaki 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 [7].

Cloud computing-capability maturity model

According to Schmidt and Grabski Cloud computing-capability maturity model is based on Software Engineering Institute's Capability Maturity Model (CMM), which is a well-established process improvement model [8]. 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 [8].

IT-Capability Maturity Framework (IT-MCF), on which Schmidt and Grabski quotes as establishing an archetype of the maturity level of an organization as it implements, improves and controls IT capabilities to support organizational value creation [8]. Identify the specific factors to be considered as

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

Schmidt and 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

- CCM Levels
- Cloud computing capability areas
- Cloud computing types

Maturity levels

CC-CMM proposes 5 maturity levels; building on maturity model is based on Software Engineering CMM.

- Organizations haven't addressed risks associated with cloud computing
- This has been termed as demarcation level by Schmidt and Grabski [8]. At this level, the organization has formalized assessment of cloud computing risk management. The risk management process is understood throughout the organization.
- 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.

Cloud computing capability areas

- Schmidt and 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.
- Schmidt and 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. Author state that an organization must determine its risk appetite and overall Enterprise Risk Management (ERM) approach.
- Schmidt and Grabski quote that management capabilities are based upon the general recommendations for cloud computing. Schmidt and Grabski says that this should include specification of how data will be migrated to and from the cloud [8]. 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.
- 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.
- 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.
- This addresses differences between the application types, that an organization might place into the cloud, and the required performance levels and required support.
- 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.

Research methodology

This study used mixed mode approach of both qualitative and quantitative methods. Additionally, this research was exploratory in nature. The qualitative research provided in-depth explanations, respondent's experiences, opinion and knowledge while the quantitative research approach provided statistical data. Both techniques were to draw from their strengths and minimize the weaknesses of quantitative and qualitative research approaches hence increase validity and reliability of the data collected. 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. The sampling frame for this study was a purposeful sample of the major cloud computing stakeholders in the University College. 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. This questionnaire was sent electronically using Google Forms [9-11].

RESULTS AND DISCUSSION

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).

Strategic alignment of cloud computing and higher education learning objectives

This research sought to establish whether there's a strategic alignment of cloud computing and the overall higher education learning objectives. From the responses, there's a clear strategic alignment of cloud computing objectives and the higher education learning 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 (Table 1).

Higher education case for cloud adoption: This research sought to establish the main reasons why the organization adopted or plans to adopt cloud computing services. 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, and gain competitive advantage through implementation of cloud-based Customer Relationship Management (CRM) and Social Relationship Management (SRM) systems. They also said 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).

Table 1: To analyse the demography of the respondents.

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

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. Most respondents confirmed that cloud computing has contributed to the achievement of business objectives. The responses received are as below.

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. 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. 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. 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 there exist such strategies. They mentioned strategies like rolebased 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 respondents 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.

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.

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.

Recommendations

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.

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.

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.

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 reminisce 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 reminisce 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. 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.

CONCLUSION

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

1. Computing GI. Gartner-IT Glossary-Cloud Computing. 2013.
2. Abbadi IM, Martin A. Trust in the cloud. Inf Secur Tech Rep. 2011; 16: 108-114.
3. Mell P, Grance T. The NIST definition of cloud computing.
4. Choudhary V. Software as a service: Implications for investment in software development. IEEE. 2007.
5. Ramesh RK, Kumar PV, Jegadeesan R. Nth third party auditing for data integrity in cloud. Asia Pac J Res. 2014 ; 1.
6. He Y. The lifecycle process model for cloud governance. Master's Thesis. 2011.
7. Saidah AS, Abdelbaki N. A new cloud computing governance framework. Closer. 2014; 671-678.
8. Schmidt PJ, Grabski SV. Proposing a cloud computing capability maturity model. 2014.
9. Badger L, Grance T, Patt-Corner R, Voas JM. Cloud computing synopsis and recommendations. National Institute of Standards & Technology. 2012.
10. Bibi S, Katsaros D, Bozanis P. Business application acquisition: On-premise or SaaS-based solutions. IEEE. 2012; 29: 86-93.
11. Nonaka I. A dynamic theory of organizational knowledge creation. Organization science. 1994; 5: 14-37.