International Research Journal of Engineering Science, Technology and Innovation Vol. 7(4)pp. 10, August, 2021
Available online https://www.interesjournals.org/engineering-science-technologyinnovation.html

Review Article

Cloud Computing Governance Readiness Assessment: Profiling Turkana University College, Kenya

Jeremiah Osida Onunga*

Tutorial Fellow & Chairperson of Department, Department of Renewable Energy & Technology, Turkana University College, Kenya

E-mail: jerryosida@gmail.com

Abstract

As a tool and as a service, Cloud Computing makes the dream of computing a reality. With its immense strength and benefits, this internet-based ongoing technology that has offered flexibility, capacity, and processing power has realized the service-oriented philosophy and has established a new ecosystem in the computer world. Cloud computing is transforming the Information Technology (IT) industry by allowing businesses to have more cost flexibility by purchasing a service rather than owning their assets. This will allow universities to move their processing and storage to the cloud, making it easier for students to access. Nonetheless, IT decision-makers struggle to evaluate Cloud services because there are no recommendations or a structured form to utilize when deciding which Cloud services to adopt. Cloud computing has emerged as a critical platform for companies looking for new methods to save money while also improving the reliability and value of their information systems. To gain the many benefits of cloud computing, an organization must have a clear cloud governance framework in place, which must be upgraded regularly to accommodate new cloud computing concerns. Many cloud users have extended their IT governance frameworks to their cloud services, yet these frameworks are insufficient in addressing governance concerns in cloud environments. Furthermore, because most consumers lack quantitative tools to assess their cloud computing governance maturity, they may miss opportunities to improve their cloud governance frameworks and achieve a better maturity level.

This study evaluated Turkana University College's cloud computing preparedness by analyzing the many opportunities and difficulties that cloud computing poses to the university. The University College employed path analysis to determine the many aspects that contribute to and impact effective cloud governance, as well as the level to which they influence it. In this research, I suggested a model for evaluating Cloud services based on a set of thirty measuring criteria divided into six groups. I demonstrated Google Apps and Microsoft Office 365 to evaluate this proposition. I conducted interviews with clients, vendors, and Cloud service professionals. In addition, I highlighted numerous main elements in cloud computing performance and examined and evaluated cloud performance in various scenarios while taking these factors into account. The results of the path analysis and the established criteria model were utilized to determine the University College's cloud computing maturity level

Keywords: Cloud computing, Readiness, Governance, Performance, Assessment, Turkana University College.

INTRODUCTION

Cloud computing has emerged as a critical platform for businesses and institutions of higher learning looking for new methods to save money while also improving the reliability and value of their information systems. Across the business, academic, and public sector spectrum, organizations are either going to the cloud or considering the cloud [1]. It provides organizations with advantages such as improved server utilization, cost savings to clients by converting Capital Expenses (CAPEX) to Operating Expenses (OPEX), dynamic scalability of IT power for clients, shortened development lifecycles for new applications, or deployments, and shortened time requirements for new business implementations.

“A model for enabling ubiquitous, convenient, on-demand,

and network access to a shared pool of configurable computing resources that may be promptly supplied and released with minimal administration effort or service provider interaction," according to NIST 800-145.

For cloud success, there are several elements to consider. Cloud computing is defined by three pillars, according to Agile Path, a famous IT research firm: cloud-centric leadership, cloud governance, and cloud administration. Every new piece of technology, according to the Agile route, generates a vacuum in the form of important IT disciplines that will aid in the acceptance, insertion, and production of value from that new technology. With new technology, IT acquisition processes are typically stretched. Early users of new technology typically fall behind in terms of industry norms. For such technologies, proven procedures and direction are constantly lacking.

According to Oracle, the cost of operating and administering applications consumes more than 75% of the annual IT budget [2]. According to Gibson, et al., it is difficult to determine whether or not those applications are truly adding value to the enterprise [3]. They go on to say that this leads to the IT application redundancy problem, in which similar IT applications produce equivalent business functionality. As a result, Tan, et al. propose that application rationalization is one option to untangle this problem. They claim that cloud services (SaaS) are a viable cost-cutting solution, especially when rationalized applications are relocated to the cloud. According to Gartner by 2015, the market for on-demand applications would be worth USD 22.1 billion, with an annual compound growth rate of 17.2 percent from 2012 to 2015 [4].

Multi-tenancy, elasticity, resource sharing, and on-demand provisioning are all properties of Cloud Computing that have the potential to complicate traditional IT operations [5]. Cloud Computing's economic models incentivize several tiers of suppliers and clients within a single virtual infrastructure, increasing the attack surface area. There is no longer a perimeter, and there are no firewalls at the Internet gateway to prevent intruders from gaining access to other systems. In cloud computing environments, it's not clear how to coordinate proper and efficient incident response without disrupting other customers' activities or breaching laws and contractual commitments. More importantly, most firms have not adjusted their IT processes for cloud services, such as incident management, event management, problem management, and change management. Instant access to cloud computing combined with direct access to the provider may allow governance mechanisms to be bypassed, exposing the company to a variety of hazards.

This paper approaches the synthesis of chitosan/PVP hydrogels with different rates between chitosan and PVP. There is also a discussion about how these hydrogels can be used in 4D printing and how bio-mimicry can contribute to this.

REVIEW OF LITERATURE

Cloud computing

Cloud computing has sparked a lot of interest in higher education research and practice as a new paradigm in information technology [6]. Various agencies and people, such as Gartner, Forrester, IDC, NIST, and ACM Communications, have defined cloud computing. Cloud computing is defined by the National Institute of Standards and Technology (NIST) 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).

Cloud computing, according to Abadi, entails the delivery of IT services through a network such as the internet. Cloud computing is defined by Seaton, a principal analyst at Forrester, as standardized IT capabilities (services, software, or infrastructure) offered through the internet in a pay-per-use, self-service manner [7].

To summarize, many researchers and institutions have attempted to define cloud computing in a variety of ways; however, as Irion., K points out, cloud computing is a departure from traditional computing in terms of storage location, hardware ownership, software delivery, interfaces to other systems, business processes, and personal collaboration [8]. As a result, it's difficult to pick out a single definition as the finest. The NIST definition of cloud computing will be used since it fits the scope and objectives of this study.

Characteristics of cloud computing models

Cloud computing has the following qualities, according to the Dallas Chapter of the Institute of Internal Auditors (2012).

Unilateral provisioning of computing resources (i.e. server time and network storage) is accomplished automatically, without the need for human interaction with a service provider, in on-demand self-service.

Broad network access

Thin and thick client platforms, such as mobile phones, tablets, laptops, and workstations, provide access to cloud services through the internet from anywhere and at any time.

Resource pooling

Cloud computing entails multi-tenancy, in which distinct physical and virtual resources are dynamically assigned and reassigned based on customer demand.

Rapid elasticity

The compute resources can be ramped in and out, up and down, in response to demand.

Measured service

Resource utilization can be tracked, regulated, and reported, giving both the provider and the user of the service transparency [9].

Cloud computing services Models of Delivery

IaaS (Infrastructure as a Service): This is a service model in which computational resources (such as processing, storage, and networks) are provisioned through the internet (NIST, 2010).

Platform as a Service (Paas): This cloud service paradigm entails providing the option for users to install their apps to the cloud using provider-supported programming.

SaaS (Software as a Service): It is a service delivery paradigm in which a client is given access to a provider's software applications that are hosted on a cloud infrastructure. SaaS is also known as "On-Demand Software Services," according to Ramesh et al., [10]. A SaaS application's security, availability, and performance are all managed by the seller [11]. Choudhary anticipated that SaaS would increase at a rate of 50% per year [12].

Models for cloud implementation

Private Cloud: This is a cloud deployment strategy in which a single organization owns the infrastructure. The organization maintains its auditing principles and methods in this paradigm [11].

The term "public cloud" refers to a cloud deployment model in which services are made available over public networks and are open to the general public [10]. Unlike private clouds, this cloud deployment architecture lets users connect to other clouds, and the number of users who can connect to this cloud is mostly limited by the capacity of the service provider [13].

Hybrid cloud: This deployment approach includes two or more of the following clouds: private, public, and community. Interface, middleware, and standard hurdles must all be addressed for a successful hybrid cloud deployment [14]. For successful hybrid cloud implementation, integration of varied interface cloud environments from different organizations and third-party vendors diverging to a homogeneous interface for end-users must be achievable.

CLOUD GOVERNANCE

IT governance, which is a component of corporate governance, includes cloud governance. Cloud governance, according to Saidah and Abdelbaki, is a framework that is implemented securely to all relevant parties and business processes to ensure that the organization's Cloud meets the aims of the organization's strategy and objectives [15]. IT governance, which is concerned with IT procedures and supports an organization's business goals, is included in corporate governance. He defines cloud governance as a framework for leadership, organizational structures, and business processes, as well as standards and compliance with these standards, that ensures that the organization's cloud capabilities support and enable the organization's aims and objectives [13].

Business growth, cost-effectiveness, asset utilization, and business agility are all deliverables of IT governance [16]. These deliverables, according to Weill and Ross, assist firms in strategically integrating business with business. IT governance must be integrated as firms attempt to utilize cloud computing for varied products to get the full benefits of cloud deployments.

Cloud Governance Models

Microsoft's Cloud Governance Model: The Microsoft Cloud Governance Model was created for the Windows Azure cloud platform and focuses on policy management [17]. Design time governance (defines service policies, quality of standards, and SLAs), run time governance (policies are enforced, and application or service performance and compliance are constantly monitored), and change management governance are the three key components of this paradigm (tracks the change activities and assets; provide and manage report, alert, and log). These three components, according to He, work together to achieve proper versioning, scaling, and security compliance.

Guo's Cloud Governance Model: Several researchers have identified this paradigm as the first academic model for cloud governance [13,15]. It covers a wide range of topics related to cloud governance [13]. Cloud governance, security, policy, and risk and compliance management were the four goals that guided its development. The components of cloud governance are divided into three groups in Guo's model: policy, operational, and management activities.

Saidah & Abdelbaki Model: According to Saidah and Abdelbaki, the cloud governance process ensures that all stakeholders' interests are protected. They do concede, however, that achieving a governance model's implementation plan that is agreed upon by all parties is a challenge. As a result, they recommend that all models and business cases use an elastic and adjustable model. They go on to say that the model must allow for movement between service providers and their customers [15].

Cloud Computing-Capability Maturity Model: The Cloud Computing-Capability Maturity Approach is based on the Software Engineering Institute's Capability Maturity Model (CMM), which is a well-established process improvement model, according to Schmidt and Grabski [18]. CMM has laid the groundwork for the creation of several capability models. The general CCM method is to develop a sequence of escalating capability levels by which an organization's processes, job assignments, organizational structures, metrics, and innovativeness may be assessed.

IT-Capability Maturity Framework (IT-MCF) as defining an archetype of an organization's maturity level as it deploys, improves, and regulates IT capabilities to enable organizational value generation. According to Schmidt and Grabski, the following elements should be considered: Level of management control and audit visibility into the cloud; CSP internal controls; and independent audits of the CSP, such as SSAE 16 and ISAE 3402 [18].

Because critical applications may be hosted in the cloud, risk assessments, controls, and assurance, as well as operational service level agreements and plans for external auditing, according to Schmidt and Grabski, should be a key component of the initial cloud computing planning and contracting process. CC-CMM has three dimensions: Cloud Computing Capability Areas and Cloud Computing Types; CCM Levels

Maturity Levels: CC-CMM proposes five maturity levels, based on Yeo and Ren Software Engineering CMM maturity model [19]. Levels 1 and 2: Organizations haven't addressed the hazards of cloud computing; Schmidt and Grabski refer to this level as the demarcation level. The organization has codified the assessment of cloud computing risk management at this level. The risk management process is well-understood by everyone in the company. Levels 4&5: At these levels, the business recognizes and incorporates major external stakeholders, including direct and indirect CSPs, such as SaaS providers and IaaS providers. The company also strives to improve its processes regularly.

Cloud Computing Capability Areas: Based on COBIT 5, Schmidt & Grabski identify six cloud computing competence categories. IT governance, management, data governance, security reliability, software applications, and technical are among these categories.

1. Information Technology Governance

According to Schmidt and Grabski, shared governance is required since it is feasible, if not likely, that IT decision rights will be transferred outside of the enterprise to the CSP. According to Rittenberg and Martens, an organization's risk appetite and overall Enterprise Risk Management (ERM) approach must be determined [20].

2. Management

Schmidt and Grabski and Badger et al., management capabilities are based on generic cloud computing suggestions [21]. According to Schmidt and Grabski, this should include details on how data will be moved to and from the cloud. Data retrieval plans, CSP's plans for continuity of operations and redundancy, SLAs that specify remediation in the event of failure, CSP's compliance with controls (as determined by third-party audits), and assurance that CSP has appropriate internal controls over their administration staff to prevent any type of security lapse are all included. The acceptable usage policy must be reviewed and vetted, as well as any additional information that may be required.

3. Data Governance

This refers to the security, integrity, and accessibility of data in the cloud. Regulatory problems and government contracts may limit data transit and storage. Other data governance concerns include how and where data is stored, ensuring that data is deleted upon exit, determining who is accountable for backups and restores, and establishing a data archiving policy.

4. Security and reliability

This ensures that only the organization's authorized users have access to the data and that the CSP can deliver the agreed-upon services based on the performance requirements defined at the outset. Encryption, physical security, authentication, and IAM approaches are all examples of security. Specification of performance standards or other Key Performance Indicators (KPIs) and having visibility into the CSP's operations in terms of an organization's data are examples of performance capabilities.

5. Software and apps

This section discusses the distinctions in the sorts of programs that a business might put in the cloud, as well as the requisite performance requirements and support.

6. Technical

This section discusses how to use virtual machines. The CSP must be able to both guard against and identify threats from other virtual machines or other sources, according to the organization. Organizations should be able to switch from one set of virtual machines to another with the same CSP or return to their premises.

Research Methodology

In this study, both qualitative and quantitative approaches were applied in a mixed-mode approach. Furthermore, this study was exploratory. In-depth explanations, respondent experiences, opinions, and knowledge were offered by qualitative research, whilst statistical data was provided by quantitative research. Both methodologies were designed to maximize the validity and dependability of the data acquired by leveraging their strengths and minimizing the limitations of quantitative and qualitative research approaches. The main tool used in this investigation was a questionnaire. The questionnaire questions were set up in a Likert scale format, with a 1 to 5 range (1: strongly disagree, 5: strongly agree). The open-ended questions in the Focus Group Discussion guide were included in the questions. The study's sampling frame was a representative sample of the University College's primary cloud computing stakeholders. Senior IT managers (including IT directors, IT security managers, and MIS managers), cloud computing users (systems analysts, systems administrators, systems developers, and IT infrastructure specialists), and business executives who participate in making IT-related decisions were the focus of the study.

RESULTS AND DISCUSSIONS

Analysis of responses for constructs measuring statements

The questionnaire used a Likert scale with five alternatives ranging from 1 to 5 ((1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly Agree)). The first two (strongly disagree and disagree) were combined into disagreeing during analysis, while the last two were mixed into agreeing, yielding three measures (agree, disagree, and neutral).

Strategic alignment of cloud computing and higher education learning objectives

The goal of this study was to see if cloud computing and general higher education learning objectives are strategically aligned. According to the comments, there is a clear strategic connection between cloud computing goals and higher education learning goals. 70 percent of respondents agreed that cloud computing goals are strategically aligned with overall corporate goals, while 16 percent disagreed and 14 percent were undecided. The study went on to look at the demographics of the respondents to see whether there was any strategic alignment. The responses were distributed as follows in the (Table 1).

Higher education case for cloud adoption

The goal of this study was to figure out why the company chose or plans to choose cloud computing services. The respondents said that by implementing cloud-based Customer Relationship Management (CRM) and Social Relationship Management (SRM) systems, they have achieved or will achieve cross-border trade and product markets, improved employee productivity through value creation, and gained a competitive advantage. They also stated that using cloud services has allowed the company to reduce IT operating costs, primarily by transforming IT Capital Expenses (CAPEX) to Operating Expenses (OPEX) as shown in (Table 2).

The researcher went on to ask whether cloud computing has aided the organization in accomplishing its overall business objectives, to determine whether cloud computing has met the objectives of its adoption in the firm. Cloud computing has aided in the attainment of company goals, according to the majority of respondents. The following are the responses shown in (Table 3).

Table 1: Strategic alignment of cloud computing responses.

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

Cloud computing value measurement

The researcher wanted to know if there are any systems in place in the organization for assessing the usefulness of cloud computing vs the hazards it poses to the company. Annual Net Present Value (NPV) and Return on Investment (ROI) reports of cloud services, cost savings from hardware support, software license and hardware purchasing, and cost reports compared to the budget allocation for cloud computing are among the measuring methodologies suggested.

Awareness of investments to be lost due to cloud adoption

When asked if the organization had considered any investments that had been lost or might be lost as a result of cloud computing adoption, the respondents said no. These investments were characterized by the respondents as some IT roles and processes, as well as control over sensitive data.

Resource Management

Questions concerning human resources and computational resources were asked under resource management. The respondents have questioned if the organization has enough skilled staff to enable cloud computing. Although some respondents agreed that skills for managing cloud services exist, the majority of respondents stated that skilled labor is still scarce or insufficient and that available resources require appropriate training to support cloud services.

Table 2: Higher Education Case for cloud adoption.

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 Productivity	91	9	0
Improve Products Or Services	27	67	6
Reach New Markets	27	68	5
Gain Competitive Advantage	95	5	0

Table 3: Cloud computing contribution towards HE objectives

Contribution towards Higher Education 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

Data Access Management

The respondents were questioned if there is an identity management strategy that governs access to cloud data as a data access management control. Such tactics, according to the respondents, do exist. For both on-premise and cloud services, they identified solutions such as role-based user access, data governance policies, multi-factor authentication, and IAM policies. They also stated that the existing cloud services adequately support identity management solutions.

According to the answers, the CSP has measures in place that allow customers to control who has access to their data. Security Content Automation Protocol (SCAP) is the most commonly used mechanism, followed by logging mechanisms, IP address range controls, Active directory policies, server, and database administrator access management, multi-factor authentication, access control lists, and communication through ports on a need-to-know basis, according to the researchers. During the setup of the MV/storage service, the CSP also allows the customer to specify the location and backup location of its data.

Cloud Computing Risk Management

The respondents were questioned if both the business and IT departments are aware of the potential hazards connected with cloud computing and if there are any risk mitigation strategies in place to manage these risks. Both the business and IT are aware of the risks associated with cloud services, which they have profiled as unlimited access to user data by cloud providers, data storage location, cloud data and deletion, customers' inability to access and manage cloud infrastructures, and limited rights to access and audit the security control, according to the respondents. According to the respondents as shown in (Table 4), there is a need for rules to manage unprivileged user access, measures to ensure that customer data is erased when CSP issues hardware to another customer, and the right to invoke electronic inquiry procedures.

Cloud Service Provider Code of Practice

The purpose of this study was to see if the respondents were aware of any code of practice published by the CSP, as this is a key part of cloud computing governance. According to the responses (Table 5), CSP has created a comprehensive cloud computing code of practice. According to the replies, this has been published on the vendors' internet page, and clients must read, understand, and sign it before getting the cloud service. Before contract signing, the CSP also sends a paper copy to the client. Any policy modifications are also communicated to the clients on time.

Cloud computing security management and auditing

User Account Audit

According to the respondents, effective audit methods are used regularly to improve user account management. The user account matrix, level of adherence to standard operating processes, and disabling accounts of employees

Table 4: 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

Table 5: Security Management summary.

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

who have left the organization are all part of the audit process. In addition, these audits verify that only authorized users have access to specific systems.

Authentication

According to the respondents, controls for managing the hazards associated with ubiquitous access have been discovered. Controls such as multi-factor authentication, access control lists, data encryptions, role-based access, digital signatures, time stamps, and trail audits were discovered and implemented to prevent cases of ubiquitous access, according to the researchers. To a considerable extent, the cloud service has accomplished these control needs, ensuring that dangers are avoided. The respondents also mentioned that these controls have provided a higher level of assurance of user authentication for cloud services platforms.

Third-Party Audits on CSP Platform

The answers answered that there is a provision in the CSP terms and conditions for a third party to audit the implementation and management of security control measures on a formal request as mentioned in the contract scope and during the vendor evaluation phase. Even though it has not been implemented, there is a written agreement in place. According to the responders, the CSP enables the service and its supporting infrastructure to be scanned for vulnerabilities and penetration tested. These tests can be performed on a quarterly, semi-annually, or annual basis by the organization itself or with the assistance of a third party. However, in the event of a threat alert, it is occasionally used as a reactionary response.

According to the respondents, the CSP has been transparent in providing audited reports from their external auditor for third-party vendor verification before the implementation of the cloud service and for subsequent reviews. The request for these reviews is spelled out in the contract agreement, and once completed, the respondent's organization follows through on the recommendations for new implementation and areas for improvement for proper closing.

Client Reference Checks

The respondents acknowledged that the CSP provided them with contact information for their present clients during CSP reference checks. According to them, vendor selection is a required stage, and procurement process management of I.C.T service providers is a critical component. They claim that reference checks are the foundation of benchmarking to ensure that the organization's scope of implementation and selection of a credible CSP is not compromised.

Availability of published cloud computing code of practice

The CSP has published a comprehensive code of practice for cloud computing. According to the replies, this has been published on the vendors' internet page, and clients must read, understand, and sign it before getting the cloud service. Before contract signing, the CSP also sends a paper copy to the client. Any policy modifications are also communicated to the clients on time.

Data Encryption

In terms of data security, the respondent stated that encrypting data is a joint duty between the enterprise and the CSP. The client is solely responsible for the security of data at rest, as the CSP just supplies infrastructure, while data in transit is encrypted by the CSP. However, they stated that if the client is unable to encrypt data at rest, the CSP can do so using formally verified encryption techniques such as AES-256 and IS 27001, with the encryption key maintained by the CSP.

Audit Recommendation Implementation

Implementing the audit advice, according to the respondents, is a joint obligation between the cloud service provider and the organization. They stated that SaaS issues would be addressed by the corporation, whereas IaaS issues would be handled by the CSP. The timelines for implementing these recommendations are based on the existing SLA established at the time of contract signing.

Service Level Management

According to the replies, the SLA is published on the management portal. To ensure that they continue to please its clients, the CSP strives to meet and surpass the specified SLA standards; this gives them an advantage during reference checks. They also stated that the IS Service Delivery Manager is solely responsible for ensuring that the SLA is met by examining the weekly systems availability report as well as the third-party availability monitoring tool. After that, the manager compares these reports to the agreed-upon SLA targets to determine whether the SLA was reached or not. CSP's SLA performance was regarded as satisfactory by the majority of respondents.

The (Table 6) below shows the summary of responses regarding Service Level Management:

Incident and Configuration Management Processes

According to the respondents, the functions of incident management, configuration management, and service desk are critical in cloud service operation, management, and governance. They claimed that the service desk provides round-the-clock support for cloud service incidents and requests, that incident management aids in the alignment of incident resolution protocols, and that configuration management aids in the setting of user accounts and licenses.

Cloud Service Monitoring

The respondents were asked if there are any different cloud service measurement methodologies. They stated that the CSP's availability and SLA performance are measured using a variety of methodologies. An on-premise monitoring tool that can monitor cloud services, and an availability monitoring tool on the cloud customer site that provides a dashboard with multiple service availability reports and various CSP-generated data that can be retrieved on demand are among the mechanisms listed.

Cloud Service Change Management

In response to the question of whether the organization has a change management procedure, the respondent stated that it does. They claim, however, that it does not adequately cover cloud service transition protocols and requires significant revision. They claimed that changing this procedure should be done in a collaborative effort involving both the business and the CSP. There are no exceptions to the change process being the primary governance of change management.

Backup and Recovery

For Software-as-a-Service, the CSP provides backup and recovery services (SaaS). Backup is the client's duty for Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Backup and recovery services, on the other hand, can be supplied by the CSP as an add-on service for PaaS and IaaS.

In response to the question of whether the CSP has mechanisms in place to ensure that client data does not travel to geographical areas prohibited by the client, respondents stated that the CSP is responsible for both data at rest and data in transit in SaaS, making it difficult to control or monitor data movement. In PaaS and IaaS cases as shown in (Table 7), 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 a proscribed geographic location.

Exit Strategy

Responses indicate that the organization has a clearly defined cloud exit policy. There also exist various measures as shown in (Table 8) to ensure that data is completely removed from the CSP servers. However, there is a lack of assurance on the measures the CSP has in place to ensure

Table 6: Service Level Management.

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

Table 7: Backup and disaster recovery summary.

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

Table 8: Summary of Exit Strategy responses.

Contribution towards HE 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 the 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 their data from the cloud	60	40	0
A third-party audit is allowed to ensure complete removal of data upon exit	3	63	33

that data is completely wiped of the cloud environment upon exit.

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 the 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.

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 the 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 the 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 a lack of visibility of the data backup location, especially for SaaS services. The organization should therefore insist on a backup and recovery plan from the CSP, including the backup and recovery sites, 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 cloud services. However, there is a 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 remain 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.

Recommendations for further research

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 assumed that the perfect correlation between the 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

Trivedi H (2013). Cloud computing adoption model for governments and large enterprises (Doctoral dissertation, Massachusetts Institute of Technology).

Oracle (2009). An oracle white paper in enterprise architecture, the oracle enterprise architecture https://www.oracle.com/technetwork/topics/entarch/oea-framework-133702.pdf

Gibson J, Rondeau, R, Eveleigh D,and Tan Q (2012). Benefits and challenges of three cloud computing service models. In 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN) (pp. 198-205).

Gartner (2013). Gartner IT Glossary-Cloud Computing. http://www.gartner.com/it-glossary/cloud-computing/

Cloud Security Alliance (CSA, 2010) Cloud "Readiness Consulting Services" http://www.cloudsecurityalliance.org/

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

Abbadi I.M, and Martin A. (2011). Trust in the Cloud. Information

Security Technical Report.16: 108-114.

Irion K. (2012). Government cloud computing and national data sovereignty. Policy & Internet, 4: 40-71.

Grance T, & Mell P. (2011). The NIST Definition of Cloud Computing. https://www.rickscloud.com/how-cloud-computing-could-help-the-aviation-industry/

Ramesh, R.K Kumar, P. V., & Jegadeesan R. (2014) "Nth Third Party Auditing for Data Integrity in Cloud". Asia Pac. J. Res.

Salesforce C. P. Q. (2009). Salesforce. Cloud CRM Solutions [online].

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

He Y (2011) The Lifecycle Process Model for Cloud Governance. University of Twente. https://www.rickscloud.com/how-cloud-computing-could-help-the-aviation-industry/

BITKOM 2009 Cloud Computing-Evolution in der Technik, Revolution im Business. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Saidah Ahmed, and Abdelbaki (2014). "A New Cloud Computing Governance Framework," CLOSER 2014, 4th International Conference on Cloud Computing and Services Science.

Weill, Peter and Ross, Jeanne W., It Governance on One Page (November 2004).SSRN: https://ssrn.com/abstract=664612 or http://dx.doi.org/10.2139/ssrn.664612

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

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

Yeo A C, Rahim M, & Ren Y Y (2009). Use of Persuasive Technology to Change End-Users' IT Security Aware Behaviour: A Pilot Study. Int. J. Hum. Soc. Sci. 4: 673-679.

Rittenberg L, and F. Martens (2012). Understanding and Communicating Risk Appetite.

Badger L, Grance T, Patt-Corner R, Voas, J (2012). Cloud Computing Synopsis and Recommendations. National Institute of Standards & Technology Special Publication. 800-146.