ASSESSING THE EFFECTIVENESS OF AN IT GOVERNANCE PRACTICES WHEN ADOPTING CLOUD COMPUTING

KWETE MWANA NYANDONGO
UNIVERSITY OF JOHANNESBURG, APPLIED INFORMATION SYSTEMS, SOUTH AFRICA
KWETEN@UJ.AC.ZA

NOSIZWE MXOBO
University of Johannesburg, Applied Information Systems, South Africa
MXOBO27@GMAIL.COM

ABSTRACT

The worldwide use of cloud computing has caused academics and professionals to become interested in studies around benefits and risks of cloud computing. Despite known risks like data security and loss of data control, cloud computing has attracted many organisations due to cost benefits and scalability. Because of this together with other factors organisations do not pay enough attention to how cloud computing affects the governance of information technology and the effect on existing security policies, business processes and service-level agreement regulations. This study explored the effectiveness of information technology governance's practices when adopting cloud computing at organisational level. In order to validate and evaluate the research problem, quantitative methodology was used. Primary data were collected through questionnaires that were distributed via email to professionals who adopted or who were planning to adopt cloud computing within the next three years.

The data collected were analysed using Excel. The results indicated that cloud-computing adoption brings a new approach to the governance of IT, being a more contractual than physical approach used in traditional IT systems. Additionally, IT governance enablers, such as business processes and security policies, are highly affected when adopting cloud computing. Moreover, organisations rely mostly on service-level agreements provided by cloud computing providers rather than setting service-level agreement expectations and demands at organisational level. This supports the view that strong service-level agreements are fundamental when adopting cloud computing and new technology, which affect business processes. This research study concluded that IT governance is critical and useful when adopting cloud computing. However, existing IT and specifically designed cloud computing governance frameworks lack to address cloud-computing components holistically. Thus, there is still a need for future studies to design integrated IT governance frameworks and further examine the practical implementation of existing frameworks in cloud computing.

Key words: Cloud computing; Effective IT governance framework; Cloud governance; Service-level agreements

INTRODUCTION

Information technology (IT) has evolved considerably since its inception in the 1960s to ensure that cost-effective, high-performance, globalised, agile and minimal human intervention technologies are provided to consumers (Speed 2011). As a result, organisations develop systems that are more flexible, quick to deploy and more responsive to customer demands (Khalil, Fernandez & Fautrero 2016; Speed 2011). The quest to speed up innovation has been the driver for organisations to acquire new technologies to meet consumer needs and to gain a competitive advantage. It is in this context that organisations worldwide are experiencing a wave of new technologies entering the market. One of these technologies is cloud computing (CC). CC offers flexible, scalable and cost-effective IT infrastructure and services accessible anywhere through the Internet. Makori (2016) claimed that CC is the best technology ever since the introduction of World Wide Web technology. Previous studies predicted that CC would become the fifth utility after electricity, water, gas and the telephone (Buyya, Yeo, Venugopal, Broberg & Brandic 2009; Subhas & Arka 2010).

CC provides economic value to all types of organisations, which can only be beneficial to a developing country such as South Africa. However, risks have been associated with CC. Potential risks could relate to governance, security, compliance with regulations, privacy, control and ownership of data. This have caused many organisations to be reluctant to implement CC services (Ahmad & Janczewski 2011; Khalil *et al.* 2016). Despite these risks and concerns, the majority of businesses in South Africa (SA) have adopted CC services. Such services range from personal emails to social media, and from IT servers to IT applications. The adoption of CC increased by 86% between 2012 and 2017 in SA (Charles & Jean-Paul 2012, Tullet 2017)

Numerous studies have been done on IT governance and CC as separate subjects but very few studies have been conducted on the relationship between IT governance and CC (Khalil *et al.* 2016; Makori 2016). IT governance denotes the structures and processes organizations utilise to ensure that IT operations support the goals and objectives of the organization through leadership guidance(Arief and Wahab 2016).The purpose of this study was to examine the effectiveness of IT governance when adopting CC. Researchers sought to examine how beneficial the IT governance best practises, including decision making rights; harnessed organization structures and business processes; policies and compliance to regulatory, are when adopting CC to ensure value delivery and mitigate risks.

In order to meet the above objective of the study the following research questions were addressed:

1. What motivates organisations to adopt CC in South Africa?
2. What is the extent to which CC is practiced in South Africa?
3. To what extent does CC affect IT governance enablers?

4. How can IT governance practices resolve concerns and risks associated with CC?
5. How often do organisations set service-level objectives prior to the adoption of CC?

A literature review will be addressed in the next section, followed by the research methodology, and subsequently by research data analysis and a conclusion.

LITERATURE REVIEW

IT has become a crucial success factor for organizations. It has been therefore embedded in modern business strategy (Goosen & Rudman 2013). Organization are aware that without IT they cannot gain competitive advantage and business operations (Goosen *et al*. 2013). Therefore, the alignment of business and IT operations is important to deal with revolving IT changes and complexity encountered when implementing IT systems (Saetang & Haider 2011). IT Governance provide solutions to these issues as it sought to align IT and business strategy to ensure that IT systems deliver value to the organization and mitigate risks .

IT Governance Background

There are various definitions of IT governance but the commonality that runs throughout is that IT governance is the responsibility of the board members and executive management and it forms part of the corporate governance (ITGI 2003, Butler, R., and Butler, M.J., 2010). Essentially IT governance consists of the organizational structure, processes and leadership that provide direction to ensure IT resources support and maximise business objectives and strategies (ITGI 2003). Brown (2006) also describe IT governance as the organisational resource that directs the establishment and deployment of IT strategy. It is generally accepted that IT governance is responsible for two core functions; value delivery and mitigation of IT risks (Ahmad *et al.* 2011).

Leadership implies that board members and executive management have the responsibility to ensure that roles, responsibilities and organizational structures are clearly defined and operative to the management of IT resources to accomplish desired conduct (Butler *et al*. 2010). Furthermore, authority should be disseminated throughout organisational structures to ensure effective implementation of IT governance (Altemimi & Zakaria 2015).

The concept of organizational structures refers to “who makes decisions and who is held accountable” (Butler *et al*. 2010). In other words, organizational structure is about roles, positions and responsibilities established within the organization to control and manage IT resources. There are three types of organizational structures namely; decentralised, centralised and federated (Altemimi *et al*. 2015). In a centralised structure all IT resources management, decision rights, roles and responsibilities are owned in a central IT department. Decentralised structure consists of each department managing IT resources separately normally executed though committees. For a federate structure both decentralise and centralised are deployed. Processes include all the procedures concerning

the governance that the above organizational structures will be responsible for, based on the adopted IT governance framework which will be mentioned in the next section (Butler *et al.* 2010).

Nisrina , Edward and Shalannanda (2016) posit that IT investments are in vain when the board of directors do not provide a controlled environment to ensure that risks are reduced, and IT resources are managed properly. Likewise, De Smet and Mayer (2016) attest that in order to manage IT security risks properly, IT governance decisions should be associated with IT project investment decisions to attain the level of risk accepted within the organisation. Risk appetite is key to quantify how much should be invested in IT security. Thus, IT governance practices and mechanisms play a significant role in reducing CC risks and concerns.

How to Measure the Effectiveness of IT Governance

Effective IT governance is the result of harnessed focused areas and continuously measuring critical success factors (CFSs) of five domains in IT governance, namely strategic alignment, risk management, resource management, value delivery and performance management (Nfuka, Rusu, Johannesson & Mutagayhwa 2011]). This results in the effective use of IT for growth, or optimisation of IT resource utilisation for business flexibility.

Therefore, it is evident that every organisation, which uses IT, should have IT governance practices in place as every organisation exists to create value for stakeholders. Nonetheless, organisations still fail to implement IT governance due to prerequisite enablers, such as policies, strategies, clearly defined structures and business processes to ensure the success of IT governance. Effective IT governance depends on properly linking organisation structures, processes and other mechanisms to the business strategy (Nfuka *et al*.2011). Organisations in the same industry could adopt the very same CC services and implement the same IT governance framework, and yet yield different results.

Moreno, Paez, Chaux and Caceres (2014) and Jokonya, Kroeze and Van der Poll (2012) state that the deployment of new IT systems does not always answer to the expectations of investors. There is a gap in translating business needs into IT requirements. They note that the decision-making process to acquire or develop IT applications is the main cause for this gap. Effective IT governance delivers devices that drive management to establish incorporated business and IT plans as well as clearly defined responsibilities and accountabilities, and to measure performance of IT initiatives responding to business requirements. Therefore, IT governance practices need to make sure IT supports business goals while maximising IT investments and mitigating risks.

As the new technology with benefits and concerns that cause uncertainties to organisations, the influence of CC on IT governance needs to be assessed to provide direction for the future of IT governance. The next section explore the concept of CC and how it links to IT governance.

Cloud Computing

It is commonly agreed that CC is the service that provides access to a shared pool of IT infrastructure and technologies comprising networks, servers, storage devices, applications and other services over the Internet on a 'pay-as-you-use' basis, with minimal human intervention (Kulkarni, Alpadi, Namjoshi & Peters 2012; Senyo, Effah & Addae 2016).

While this might sound similar to outsourcing IT services to external providers, with which many organisations are familiar, CC is intended to integrate the Internet, virtualisation and automation technologies to make IT operations more efficient, standardised and cost-effective (Dhar 2012; Hon & Millard 2012). Unlike traditional outsourcing, CC is flexible and enables consumers to manage IT resources (Keuper, Oecking & Degenhardt 2011). Moreover, CC offers pre-packaged and standardised IT services, as compared to customisation done by outsourcing, in order to meet the needs of a specific organisation (Makori 2016; Mark-Shane 2009). To provide better understanding of this new technology, CC architecture has been discussed below.

Cloud Computing Architecture

CC is designed in a three-layer architecture consisting of an application, environment and infrastructure layer (Lin, Fu, Zhu & Dasmalchi 2009; Keuper *et al*. 2011). In the application layer, consumers gain access to standardised applications and software provided as software-as-a-service (SaaS) model. The environment layer provides a platform for consumers to customise and build new applications within the provided virtualised hardware, network and operating systems delivered as a platform-as-a-service (PaaS) model (Makori 2016). In both the SaaS and PaaS models, consumers do not have control over actual resources that supply support to those applications, such as the operating system, network and hardware. Finally, the infrastructure layer enables consumers to utilise actual resources on demand supplied as an infrastructure-as-a-service (IaaS) model (Kulkarni *et al*. 2012).

The CC service models are distributed to consumers in four different deployment models, to allow consumers to adopt CC services based on organisation concerns for data privacy and discretion in terms of sharing network resources. The public model provides services and is available to the general public, i.e. both organisations and individuals (Zhang, Cheng & Boutuba 2010). In the private model, services are dedicated, shared and managed within an organisation, either residing inside their premises or through a third party (Bounagul, Hafiddi & Mezrioul 2015). This type of service is especially suitable for consumers who have concerns about sharing resources and data privacy. It is, however, slightly more expensive compared to other service models (Makori 2016; Senyo *et al*. 2016).

The community model comprises organisations that have commonalities in their operations, such as strategy, mission, vision, security and regulatory compliance. Likewise, the community CC model shares similarities with the private service model. Resources can be managed and allocated by one of the involved organisations or through a third party (Shawish & Salama 2014). The hybrid

model combines deployment models for both private and public or community CC supported by standardised technology, which ensures IT applications and data are portable (Mell & Grance 2011).

The benefits of CC, which include scalability and cost-effectiveness, are derived from the five characteristics of the CC as mentioned in the National Institute of Standards and Technology (NIST) definition of CC, namely on demand self-service, resource pooling, broad network access, elasticity and measured services (Mell *et al*. 2011).

On demand self-service implies that consumers only pay for the services they consume on a subscription basis fostering cost reduction (Shawish *et al*.2014). Resource pooling presents the functionality of operating multiple IT applications in a shared physical but logically separated integrated environment (Zhang *et al*. 2010). Broad network access allows CC services to be accessed through any network device (i.e. mobile phone, personal computer) (Mell *et al*. 2011). Elasticity refers to the extent to which systems adapt to workload demand by automating the provision of network resources. In measured services, components of the CC services are monitored and controlled by the CC provider to provide correct billing and managed access control (Heier, Borgman & Bahli 2012).

The design and delivery of CC services interests all sizes of organizations because they are no longer paying for unused IT services and reduce costs on licencing fees and maintenance. Nevertheless CC, as any other new technology, has risks that might overshadow benefits (Senyo *et al*. 2016). Makori (2016) reports that close to 40% of organisations are hesitant to adopt CC services due to security risks, data confidentiality and a lack of regulations. Additionally, Alsudiari and Vasista (2012) mention that trust, transparency and regulatory requirements are difficult to manage in CC. To overcome CC risks and uncertainties, Speed (2011) propose that effective and solid governance are required to manage the adoption of CC. For this reason in the next section we discuss the importance of IT governance when adopting CC.

The Need for IT Governance in Cloud Computing

As mentioned above IT governance is about ensuring responsible and accountable management of IT resources, which consist of data, people, policies and infrastructure (Guo & Song 2010, Goosen *et al* 2013), irrespective of where the IT infrastructure is situated (Denford, Dawson & Desouza 2017). Nisrina *et al*. (2016) posit that governance assists organisations to secure and control data stored in the CC services. In addition, IT governance align the organisation with the speed of rapidly changing IT solutions and cope with market demands for new IT systems.

Essentially, for organisations to benefit from IT investments, governance should be implemented specifically in accordance with their processes, policies, culture, behaviour, organisational structure, vision and mission, which are known as factors that influences IT governance (Nfuka *et al.* 2011). Thus, it is imperative to have governance framework when setting criteria and policies that will guide the

acquisition, operation and management as well as direct decision-making because CC services impact business processes (Bounagul *et al*. 2015) – and IT governance provides this structure. Guo *et al*. 2010 emphasise that organisations must have deployed IT governance framework to ensure adopted CC services are utilised according to approved policies and procedures

Various organisations and researchers have proposed brilliant, resourceful and convenient governance frameworks specifically for CC focusing on certain CC elements, such as network infrastructure and security (Jol 2014), but these frameworks fail to address CC concerns holistically and are difficult to integrate with IT governance practices (Bounagul *et al*. 2015). The below table (*table 1*) represent different frameworks proposed for CC and IT governance at large, including worldwide accepted frameworks and research proposals.

Oliveira, Dora, Spohn and Oliveira (2015), stipulate that proper CC governance helps an organisation to optimise risk management, operations, costs and legislative compliance. It is clear that IT governance for CC is critical, though lack of integrated governance framework is also a concern for many organizations.

Governance in CC could not be effective without addressing service-level agreements, discussed in the next subsection. According to Oliveira *et al.* (2015), Heyink (2014), Buyya *et al.* (2009) and Alsudiari *et al.* (2012), the SLA is the only legal binding document and cornerstone in the CC provider and consumer relationship. It also plays a key role when it comes to governing CC services properly.

Service-Level Agreements in CC

It is evident that CC comes with different approaches of delivering, managing and servicing IT resources, focusing on contractual rather than physical aspects (Nisrina *et al.* 2016), as organisations are no longer liable for paying and maintaining hardware and software. Consequently, organisations need to transform the manner in which they govern IT resources to optimise value delivered and mitigate risks.

The SLA provides clear instructions about negotiated and agreed-upon service terms, such as billing, availability, performance and penalties when service requirements are not met (Alhamad, Dillon & Chang 2010). Additionally, a Service-Level Objectives (SLO) document is used to specify obligations and all actions should be taken when either or both CC provider and consumer do not comply with agreed service terms mentioned in the SLA.

Oliveira *et al*. (2015) mention eight SLA metrics about which service providers should be open. These metrics depend heavily on network performance or application itself, availability, storage, response time, delay, bandwidth, jitter, security and usability. Although SLA compliance metrics are compulsory, customers still do not have standardised access to them (Heyink 2014). This may result in providers over-allocating resources or avoiding to pay penalties when SLAs are not met. Khalil *et al.* (2016) add that SLAs provided by CC providers

lack transparency when disclosing details about how and where the data is stored.

Name	*Released by*	*Description*	*Limitations*
Control objective for information and related technology (CobiT)	*Information systems audit and control association (ISACA),*	*Provides IT governance domains, processes, and controls objectives; and focuses on aligning IT with business goals, providing metrics and maturity models to measure their achievement. Mapping to other models and technique and standards' ITIL and ISO.*	*Still limited to traditional in-house IT governance; and its adoption for CC governance requires the framework tailoring to reach the governance of CC.* *Banagui et al. 2015,*
ISO/IEC 27017 series	*International organization for standardization*	*The ISO/IEC27k series provide best practice recommendations on information security management and propose several publications each deals with specific security domain and most recent publication deals with information security controls, and protection of personally identifiable information for cloud service.*	*Limited to one cloud governance domain, consequently their adoption for the CC will only focus on the governance of CC information security (Arief et al 2016, Banagui et al. 2015, Goosen et al 2013).*
NIST-SP 800-53	*National institutes of standards and technology (NIST)*	*Security standard for federal information systems that provides a catalogue of security and privacy controls intended to protect organization operations, assets, and individuals from diverse variety of security threats.*	*Limited to one cloud governance domain, consequently their adoption for the CC will only focus on the governance of CC information security (Banagui et al. 2015).*
Cloud Control Matrix (CCM)	*Cloud security Alliance*	*Provides fundamental security principles and controls that guide CC providers s and assist CC consumers in assessing the security risks of CC. Based on several industry-accepted security standards, regulations, and*	*Limited to one cloud governance domain, consequently their adoption for the CC will only focus on the governance of CC information security (Banagui et al.*

		control frameworks; the CCM provides a domain centric view and constitute a mix of compliance, governance and technical controls.	*2015).*
Federal risk and authorization program (FedRAMP)	*the Federal risk and authorization program*	*Standardized approach for the assessment and monitoring of CC assets and services. Considered as the result of multiple collaborations, FedRAMP enables public agencies and industries to entrust their security assessment processes for various known security controls predefined by the framework.*	*Limited to provide guidance do not consequently provide an integrated approach for CC governance (Banagui et al. 2015).*
Guo Model	*Z. Guo, M. Song, and J. Song. Guo & Song 2010*	*Underlines the increasing need for policy schemes, service profiles, management and governance processes, particularly the need for service lifecycle management, visibility, and contextualization.*	*Attempted to address three different model's management, operational and policy, but lack transparency continuity of critical business processes is performed and integration existing IT governance frameworks. (Banagui et al. 2015, Guo 2010)*
Cloud Cube Model	*Open Group*	*Outlines the steps that organizations should follow before migrating to the cloud. Thus, the model illustrates the possible permutations in cloud offering and also the manner of them.*	*Focus on providing guidance and best practices to avoid security risks, instead of proposing a holistic approach for CC governance.*
European Union legislation Act on Data Protection Directive 95/46/EC	*Council of the European Union and European Commission*	*The regulation that aim to support and standardize data protection for all individuals with the European union(EU). It also addresses the export*	*This regulation is limited to data privacy. (Heynk 2014, Alsudiarii et al. 2012)*

		of data outside the EU.	

Table 1. IT and Cloud computing framework

Therefore, a new approach to implement IT governance, for instance planning, monitoring and control, is required to encourage transparency (Oliveira *et al*. 2015). Moreover emphasised, it is imperative for CC providers to assure that principles of availability, confidentiality, reliability and integrity are met when providing consumer's SLO's. Further, Speed (2011) mentions that critical principles of disaster recovery and the ability to retrieve data when changing CC providers are always least considered. Taken this, among other related factors into account, there is a need for regulated monitoring tools that will inform customers about the present and past performance of the service provider, to ensure correct billing.

The Law Society of South Africa adopted the European Union legislation Act on Data Protection (Sections 19 to 22) which presents information that should be included in a CC contract agreement (Heyink 2014, Alsudiari *et al*.2012) to manage legal implications of agreements between the CC provider and the consumer. The Act stipulates that an agreement contract should address compliance metrics regarding security, including availability, data location, confidentiality, integrity and accountability (Heyink 2014). In CC, trust is highlighted as one of the inhibitors preventing organisations from adopting CC services. Therefore, reflecting effective SLA compliance metrics would be advantageous to CC providers in order to attract new customers and gain customer loyalty from existing clients (Oliveira *et al*. 2015).

The challenges with which organisations are faced in terms of standardised CC governance frameworks emanate from the high pace at which CC services are developed and adoption operate. Organisations are struggling to keep records of all CC services adopted by individuals and departments. Khalil *et al*. (2016) highlight "shadow IT" as the main concern to govern CC services. The term 'shadow IT' means that each department acquires CC services without consulting the IT department. Consequently, shadow IT is the result of a decentralised IT department structure as stipulated in organizational structures. Therefore, it is the responsibility of the board and executive management to provide a governance model to ensure they protect intellectual property and control who has access to the system. Finally, the pressure to get new applications from the business also becomes a challenge for the IT department in order to conform to regulations. This study strived to determine whether IT governance is effective and efficient to encompass CC dynamics.

RESEARCH METHODOLOGY

Research Design

This study sought to explore the effectiveness of IT governance when adopting CC, by assessing the relationship between these two subjects and ascertain how CC affects IT governance. In order to achieve the objectives of this study, the quantitative approach was found to be the best suitable methodology. This approach will explain, confirm, and validate the relationship between the two different subject matters in this study, being CC and IT governance (Shields & Rangarajan 2013, Williams 2007).

Smith 2017 and Williams 2007, agree that the quantitative approach is objective and provide pure inputs from participants. As a result, this methodology proves to be fair and independent of the researcher ‘s views. Moreover, the quantitative approach provides an objective measure of reality.

The quantitative approach adopts different methods to gather data, including surveys, experimental researches and questionnaires, on predetermined instruments that result in statistical data (Williams 2007). For the purpose of this study, questionnaires were used as an instrument to collect primary data from participants who corresponded.

Data was analysed using Microsoft excel 2016. The following sections will address sampling techniques and measures utilised in this study and findings in detail.

Sampling

For the purpose of this study, participants were randomly selected from various industries (i.e. education, health, IT and others) who were planning to adopt CC, but also those who had adopted CC already. The sampling frame was based on organisations operating in South Africa. Participants were nominated on the basis of occupation and experience with CC and IT governance practices. The targeted participants comprised individuals occupying positions as IT manager, IT specialists, IT auditors, CC providers and Business process specialists. The questionnaires were distributed via email to more than 50 participants and more than 50% responded with valuable input that was used to add value to this study. Participants participated on a voluntary basis and were assured that information would be kept confidential. The reason for selecting a questionnaire as a tool to gather data is explained below.

Measure and Data collection

The questionnare is one of the commonly utilised instruments in quantitative research because it is efficient for obtaining data of a both predicted and unpredicted structure (Williams 2007) .For this rationale a standardised questionnaire was employed as tool to gather data. The questionnaire consisted predominantly of closed-ended questions and overall comment section which provided more insight for our findings. To provide trustworthy and valid results, data were analysed using Microsoft Excel 2016 functions, and the results were presented in various graphs.

Participants engaged in a self-administered questionnaire, to provide insight into their experience of adopting CC. Participants were encouraged to provide further explanation about selected option(s) rather than a tick box exercise. In addition, participants were requested to give their overall comment at the end of the questionnaire, which yielded good results. Follow-up questions were sent by email where clarity was required. A quantitative study was the viable option to provide the desired results and to respond to the challenge of participants not available for face-to-face interviews (Wagner & Moshtaf 2016).

The questions were derived from the interest of IT governance best practises of as noted in the literature review including SLA's, organizational structures, business policies and processes, as well as previous online surveys aimed at assessing benefits and concerns in the adoption of CC.

RESULTS AND DISCUSSION

The results from both primary (questionnaire) and secondary (literature review) data of the study were used as a metric to primarily measure the effectiveness of IT governance by addressing the five research questions mentioned when introducing our research statement in page 2.

The results section is categorised into three segments to address our research statement objectively. Section 2.2.1 is about CC benefits and concerns and sought to respond to questions about what motivate organization to adopt CC and to which extent CC is practised in SA. The second part present data about CC responsiveness on the cornerstone of the CC provider and consumer relationship which is the SLA. This section relates to the question about organizations' role when setting and negotiating SLA and SLO.

The latter section illustrates results about IT governance enablers that are impacted by the adoption CC. Lastly the overall comments section covers governance best practises that need to be taken into consideration when adopting CC and also clearly defines the role of the CC provider and consumer.

CLOUD COMPUTING BENEFITS AND CONCERNS

Findings of this study depict that the adoption of CC is still growing strong in various industries in South Africa. More than 45% of the participating organisations were already using CC services at the time of the study, while approximately 28% were planning to implement within the next 12 months. Figure 1 below depicts the present and future of CC service in South Africa going as far as the next three years.

CC services components comprise enterprise resource planning (ERP), mail servers, data storage and file sharing tools, which contribute mostly to the adoption of CC. Both ERP and mail servers store sensitive data that critical for business operations and decision-making. Thus SLAs are important to ensure that data can be transferred easily when a customer decides to change CC providers, such as from Oracle to SAP. The participants noted that the adoption of ERP systems eases the burden of paying enormous licencing fees, hardware maintenance and software upgrades. The ERP systems on CC make it easy to apply patches. Figure 2 illustrates the adoption of various CC components.

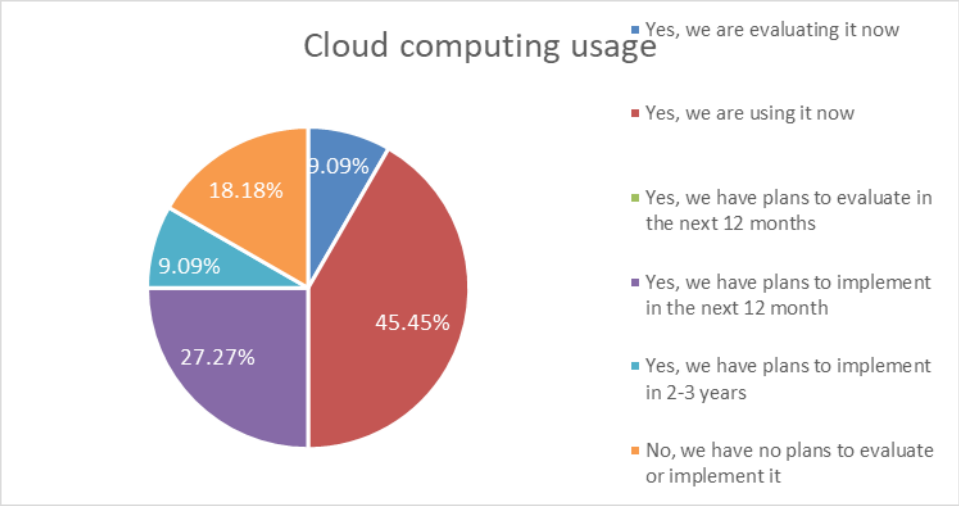

Figure 1: CC adoption in South Africa between 12 to 36 months

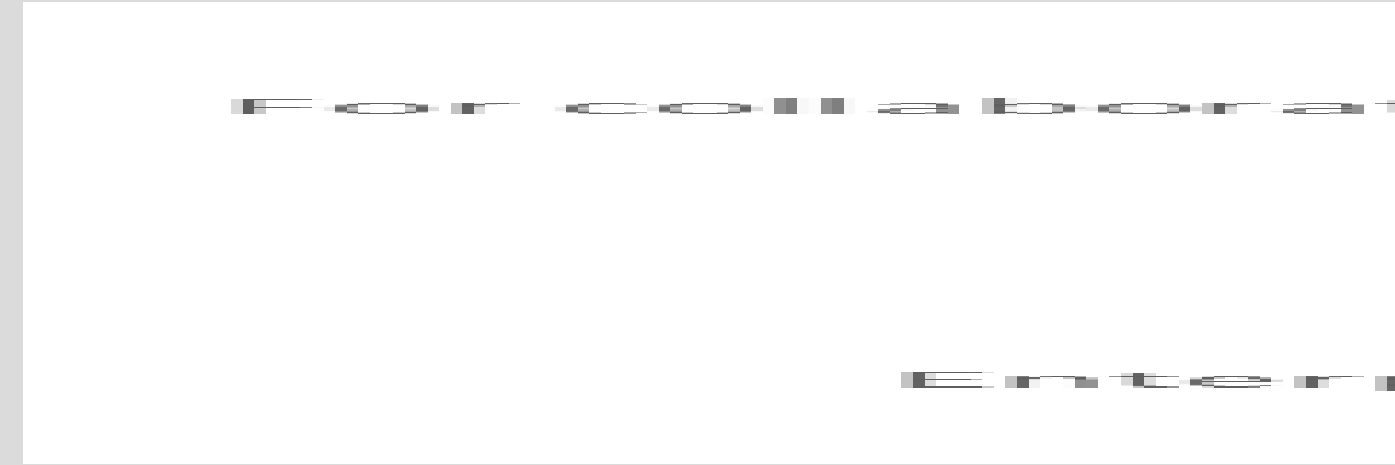

Figure 2: Most adopted CC services

Despite numerous proposed CC governance possibilities focusing specifically on security and growing numbers in adopting CC, for more than 63% of participants, security risk remained the main concern. As a result, participants planning to adopt ERP systems planned to move only data and infrastructure in non-production environments to the CC and keep the production environment on the premises. Figure 3 also shows that CC is not compatible with legacy tradition systems causing it to be difficult to integrate with in-house systems.

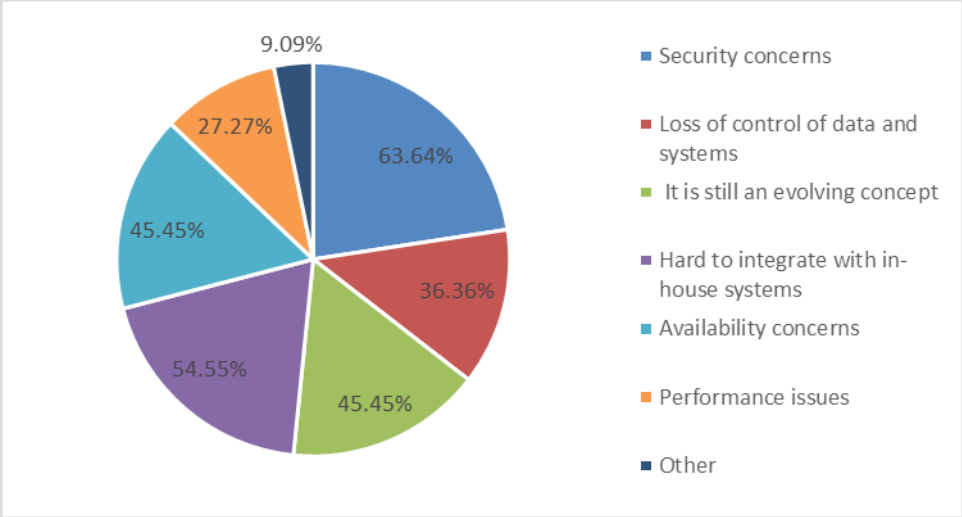

Figure 3: Cloud computing concerns

This study also revealed not well-known concerns that were hardly mentioned in previous studies as hindrances, namely compatibility with legacy systems and CC as the evolving concept, “Trust”. Trust came up as one of the concerns since CC is still an evolving concept. Furthermore, availability is still reflected as one of the main concerns.

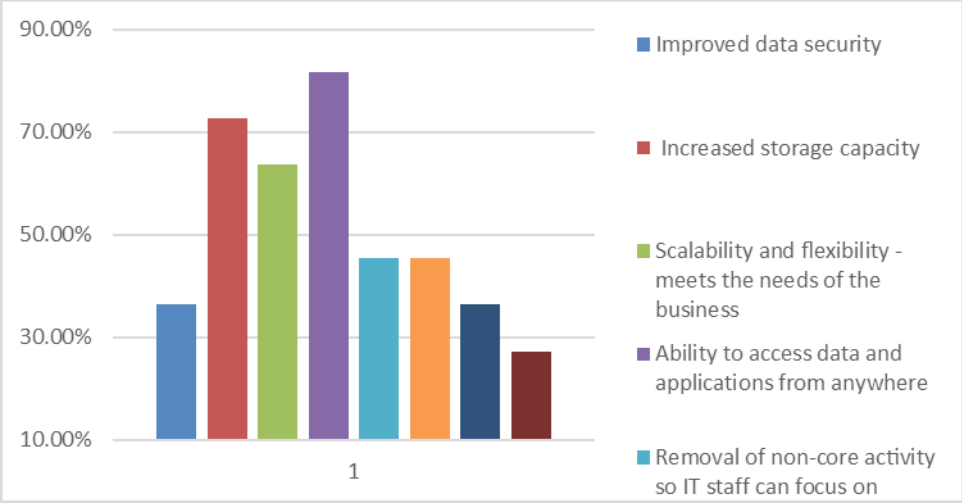

Figure 4: Benefits of using cloud computing

Besides all these concerns, benefits of the cloud are still noticeable, contributing greatly towards the growth of CC adoption in South Africa. The ability to access data and application anywhere is realised as the key benefit followed by increased storage and scalability as shown in Figure 4 above.

In addition to the benefits of the cloud, many participants indicate the main reasons that led them to the adoption of CC were to save on hardware and reduced staff costs. These findings confirm the main selling point of CC, which is saving on hardware. Figure 6 illustrates benefits that led organisations to adopt CC.

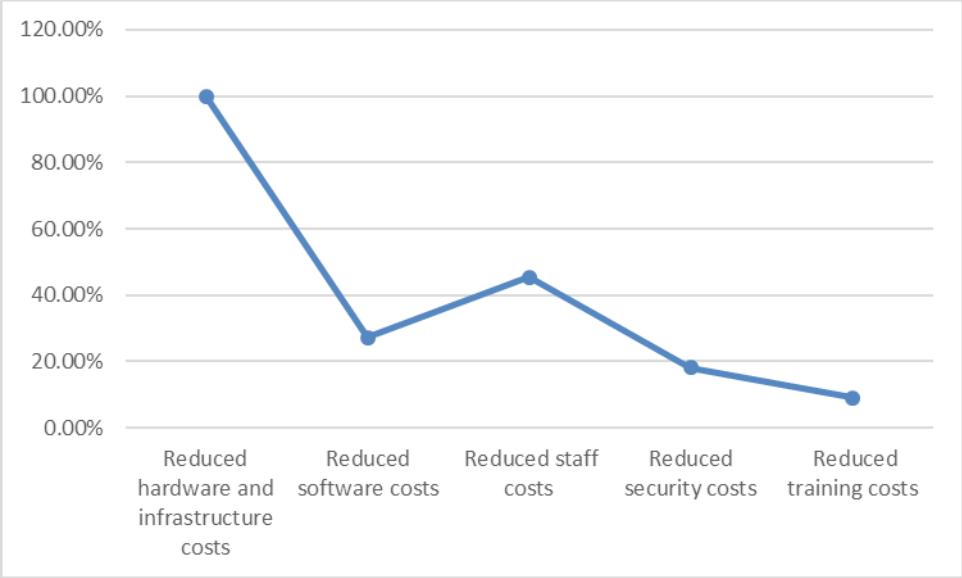

Figure 5: Benefits leading to the adoption of cloud computing

Service-Level Agreements in Cloud Computing

As indicated in the literature review, SLA is the cornerstone of a well-established relationship between the CC provider and the consumer. Yet, more than 33% of the participants indicated they did not have service-level objectives available meaning they relied on what was provided by the CC provider. Moreover, more than 41% of the participants were not sure whether the service-level objectives were available. This might be the result of a lack of awareness and training. Figure 6 depicts these figures.

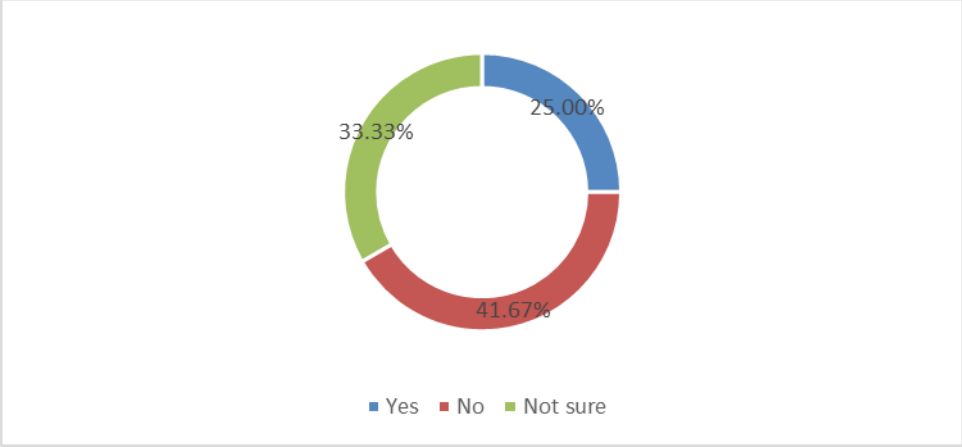

Figure 6: Setting service-level objectives for cloud computing

In the overall comment section one of CC providers participant proposed that the same governance and security principles established for the traditional IT system should apply to CC as well. Furthermore one of the most important factors for the public model CC service are physical, logical and data security. As part of the End User directive and new general Data Protection regulations, technical and

organisational measures of the CC service provider are of paramount importance.

From a physical standpoint of view it is the onus of the CC consumer to ensure that physical measures are in place to protect the data from being accessed by authorised users, including biometrics, man traps, physical security guards protecting entrance and exits and CCTV cameras. From a logical point, CC service provider is responsible to secure the IT applications, virtual and physical infrastructure, databases and storage and backup strategies. Business continuity is also extremely important.

There are also other logical security measures, such as anti-virus, anti-spam, intrusion detection systems (IDS), intrusion prevention systems (IPS) that should be in place to prevent data breaches and distributed denial of service. This supports that CC providers should disclose information about compliance metrics in the SLA (Oliveira *et al*. 2015). However, although security is assured in the SLA, participating CC consumers who are IT directors were still not clear about the security architecture and the processes as stipulated above. In addition they were not certain whether the reversibility process is addressed in the SLA.

Moreover, participating CC providers mentioned that customers who were well prepared and ready for the adoption of CC imposed their own governance policy restrictions by restricting information from crossing South African borders. In contrast, participating IT specialists and IT directors indicated that they only realised after adopting CC that they needed to take responsibility for handling data storage and usage. As a result, they were drafting policies to govern the use of CC.

Affected Enablers of Effective IT Governance

Figure 6 below is clear about the adoption of how CC affects the enablers of effective IT governance policies, business processes and ownership of data.

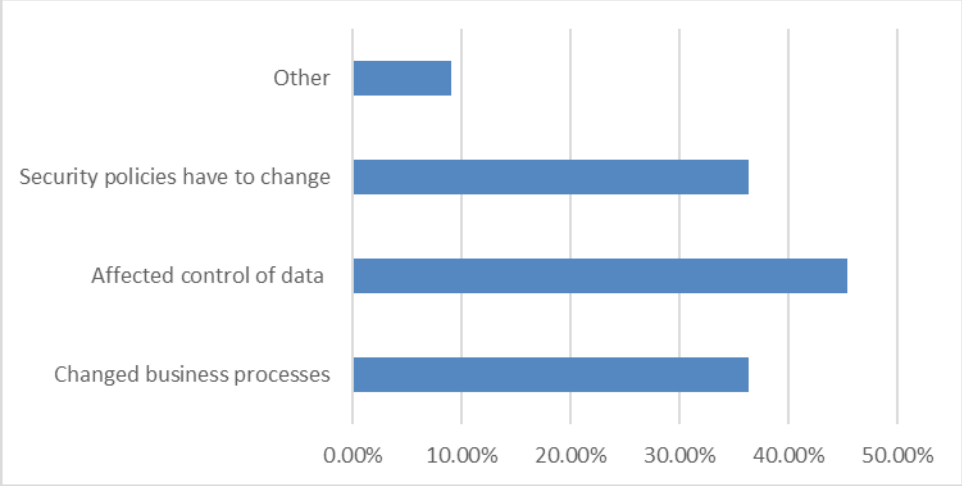

Figure 7: Affected Areas of IT governance enablers

The control of data is heavily affected, as confirmed by more than 45% of the participants. This was followed by a change in business processes and a change

in security and policies. The CC provider participant explained that, since there would be a new party involved in the handling of data, i.e. the CC provider, there would also be new policies regarding the data controller (as the consumer), the data processor (as the provider) and especially the handling of sensitive information including employees and customers information by both parties.

The CC provider further explained that data protection is most important to the customer as there are government entities and local regulators who require processes to be in place to protect personal data. This may be things like the right to be forgotten or that data cannot cross the borders of the country or the right of the data subject on storing and handling his or her personal information. In South Africa, there is a data protection law called the Protection of Personal Information (POPI) Act 2013, propagated in the Government Gazette Notice 37067 on 26 November 2013 (ISACA 2017). This Act is based on the end consumer directive and addresses the handling of the data life cycle. In addition, there are special mentioning of data leaving the country and also requirements that need to be fulfilled for any data leaving the country. This means the cloud consumer is regarded as data controller who should have policies governing the control of data. However, many organisations do not have policies in place to control the data as they depend on CC provider's SLAs.

Cloud providers also noted that cloud infrastructure within South Africa is currently relatively expensive. Applying traditional IT governance and good practice to solution design will ensure that all stakeholder concerns are addressed, and the solution deployed in an optimal environment whether it be physical, virtualised, cloud or some form of hybrid environment.

CONCLUSION

It is unarguably so that CC is the best new technology for organisations to save on hardware, maintenance and licensing costs, especially in the face of current tough economic times globally. The purpose of this study was to evaluate the benefits of deploying IT governance best practices when adopting CC. To corroborate this study quantitative approach was employed through literature review and questionnaires. The literature review reveals that governance in CC is critical however existing frameworks lack addressing CC holistically.

The result of this study demonstrate that there is a clear indication of the rise in adoption of CC services in South Africa. Regardless of undisputed uncertainties, organisations still perceive CC as the best solution. Therefore, this conform to our literature review. It remains important that the organisation balance the different concerns and benefits to ensure that there is a net benefit to using CC and that the organisation does not end up trading the advantages for other unintended disadvantages. An example might be running a certain workload on a cloud infrastructure that is more flexible, but which ends up costing more due to security measures/controls. IT governance is certain to provide framework to ensure organizations benefit from CC. Furthermore, findings in this study showed that CC consumers lack knowledge in understanding their role as data controllers and negotiating SLAs through set service-level objectives. Additionally most

organizations do not have policies in place to respond to changes brought into the business strategy by CC

In conclusion researchers believe that the objectives of the study were met, as this study managed to establish relationship between CC and IT governance and also how IT governance could be used to manage the adoption of CC. This study provides insight into and awareness on what organisations need to prepare prior to adopting CC.

The limitation of this study was the use of a quantitative approach, which might have constrained gaining in-depth knowledge as compared to using the interview technique. Nonetheless, data collected provided substantial reasons for future research to explore an integrated IT governance model that would consider IT as a service. As well as evaluating the practical implementation of existing governance frameworks. Existing IT governance frameworks in organisations should therefore be reviewed continuously to ensure effectiveness in aligning business and CC strategy.

REFERENCES

Ahmad, R., and Janczewski, L., (2011), Governance Life Cycle framework for Managing Security in Public Cloud: From User Perspective. In Proc. 4th Int. Conf. IEEE Cloud Computing, pp.372-381. United States of America: Washington

Alhamad, M., Dillon, T., and Chang, E., (2010), Conceptual SLA framework for cloud computing. In Proc. 4th Int. Conf. Digital Ecosystems and Technologies, pp. 601-610. United Arab Emirates: Dubai.

Alsudiari, T., Mohammed, A.T., and Vasista, T., (2012), Cloud computing and privacy regulations: An exploratory study on issues and implications. Advanced Computing: An International Journal (ACIJ), 3(2), 159-169.

Altemimi, M.A.H., And Zakaria.M.S., (2015), Developing Factors for Effective IT Governance Mechanism. In Proc. 9th Malaysian. Conf. Software Engineering, pp. 245 – 251. Malaysia: Kuala Lumpur.

Arief A., and Wahab, I.H.A., (2015), An integrative framework of COBIT and TOGAF for designing IT governance in local government. In Proc. 2nd Int. Conf. Information Technology, pp36-40. Indonesia: Semarang.

Bounagul, Y., Hafiddi, H., and Mezrioul, A., (2015), In Proc. 12th Int. Conf. Computer Systems and Applications (AICCSA), pp. 1-8. Morocco: Marrakech.

Brown , C.W., (2006), IT governance, architectural competency, and the Vasa. Information Management & Computer Security, 14(2), 140-154. Complementary Index database.

Butler, R., and Butler, M.J., (2010), Beyond King III: Assigning accountability for IT governance in South African enterprises. South African Journal of Business Management, 41(3), 33-45.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I., (2009), Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599–616.

Charles, H., and Jean-Paul, B., (2012), Cloud computing in South African SMMEs: Risks and rewards for playing altitude. International Research Journal of Computer Science Engineering and Applications, 1 (1), 32-41.

De Haes, S., and Van Grembergen, W., (2009), Exploring the relationship between IT governance practices and business/IT alignment through extreme case analysis in Belgian mid-to-large size financial enterprises. Journal of Enterprise Information Management, 22(5), 615–637.

Denford, S.J., Dawson, G.S., and Desouza, K.C., (2017), Exploring IT-enabled public-sector innovation in US states. In Proc. 50th Int. Conf. System Sciences, pp. 5174-5183. Hawaii.

De Smet, D., and Mayer, N., (2016), Integration of IT governance and security risk management: A systematic literature review. In Proc. 2016 Int. Conf. Information Society, pp. 143-148. Ireland: Dublin.

Dhar, S., (2012), From outsourcing to cloud computing: Evolution of IT services. Management Research Review, 35(8), 664–675.

Goosen, R., and Rudman, R., (2013), The development of an integrated framework in order to address King lll's IT governance principles at a strategic level. South African Journal of Business Management, 44(4), 91–103.

Guo, Z., and Song, M., (2010), A governance model for cloud computing. In Proc. 2010 Int. Conf. Management and Service Science, pp. 1-6, China: Wuhan.

Heier, H., Borgman, H.P., and Bahli, B., (2012), Cloudrise: Opportunities and challenges for IT governance at the dawn of cloud computing. In Proc. 45th Int. Conf. System Sciences, pp. 4982-4991. Hawaii.

Hon, W.K., and Millard, C., (2012), Cloud computing vs. traditional outsourcing: Key differences. Society for Computers and Law Magazine, 23(4), article 05/10/2012.

Jokonya, O., Kroeze, J.H., and Van der Poll, A.J., (2012), Towards a framework for decision making regarding IT adoption. In Proc. Conf. South African Institute for Computer Scientists and Information Technologists, pp. 316-325, United States of America: New York.

Jol, S., (2014), Towards a cloud computing evaluation and governance framework. Unpublished master's dissertation, Universiteit Utrecht, Business Informatics.

ISACA 2017, https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx

IT Governance Institutute(ITGI)., (2003), Board briefing on IT Governance, 2nd Edition. United States of America.

Keuper, F., Oecking, A., and Degenhardt, A., (eds.) (2011), Application Management Challenges: Service Creation – Strategies. Germany.

Khalil, S., Fernandez, V., and Fautrero, V., (2016), Cloud impact on IT governance. In Proc. 18th Int. Conf. Business Informatics , pp. 255-261. France: Paris.

Kulkarni, G., Mandhare, S., Bendale, D., Belsare, S., and Patil, S., (2012), Software as service cloud. In Proc. 2012 Int. Conf. Computer Science & Service System (CSSS), pp. 442-445, China: Nanjing.

Lin, G., Fu, D., Zhu, J., and Dasmalchi,G.,(2009) , Cloud Computing: IT as a Service.IT Professional Magazine, 11(2), 10-13.

Makori, E.O., (2016), Exploration of cloud computing practices in university libraries in Kenya. Library Hi Tech News, 33(9), 16–24.

Mark-Shane, E.S., (2009), Cloud computing and collaboration. Library Hi Tech News, 26(9),10–13.

Mell, P., and Grance, T., (2011), The NIST Definition of Cloud Computing. Special publication 800-145. Information Technology Laboratory National Institute of Standards and Technology, Computer Security Division.

Moreno, L.M.M., Paez, J.O.T., Chaux, D.A.P., and Caceres, D.A.C., (2014), IT4+: The Colombian government IT management model. In Proc. 8th Int. Conf. Theory and Practice of Electronic Governance, pp. 486–487. Portugal: Guimaraes.

Nfuka, E., Rusu, L., Johannesson, P., and Mutagahywa B., (2009), The state of IT governance in organizations from the public sector in a developing country. Industrial Management & Data Systems, 111 (9), 1418-1448.

Nisrina , I.K., Edward, I.J.M., and Shalannanda ,W., (2016), IT Governance Framework Planning Based on COBIT 5 Case Study: Secured Internet Service Provider Company. In Proc. 2nd Int. Conf. Wireless and Telematics (ICWT), pp 51-56 .Indonesia: Yogyakarta.

Oliveira, A., Dóra, P., Spohn, M., and Oliveira, K., (2015), From the dark net to the cloudy data: Cloud network governance guidelines. In Proc. 34th Int. Conf. Chilean Computer Science Society (SCCC), pp. 1 – 8, Chile: Santiago.

Saetang, S., and Haider, A., (2011), Conceptual aspects of IT governance in enterprise environment. In Proc. 49th SIGMIS Ann. Conf. Computer personnel research, pp 79-82. USA : Texas-San Antonio.

Senyo, P.K., Effah, J., and Addae, E., (2016), Preliminary insight into cloud computing adoption in a developing country. Journal of Enterprise Information Management, 29(4), 505–524.

Shawish A., Salama M., (2014) ,Cloud Computing: Paradigms and Technologies. In: Xhafa F., Bessis N. (eds.) Inter-cooperative Collective Intelligence: Techniques and Applications. Studies in Computational Intelligence, Vol .495, pp. 39-67. Heidelberg: Springer-Verlag

Shields, M.P., and Rangarajan , N., (2013), A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management , United States of America : Texas - Dallas.

Smith, T., (2017), Qualitative & Quantitative research. Research Starters Education. 4/1/2017, 1.

Speed, R., (2011), IT governance and the cloud: Principles and practice for governing adoption of cloud computing. ISACA Journal , 5 , 1 - 6.

Subhas, C.M., and Arka, M., (2010), Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding return on investment. International Journal Archive :Mathematical and Computer Modelling , 53 (3-4) , 504-521.

Tullet, J., (2017), Cloud Computing in SA – an industry update .https://www.nebula.co.za/2017/05/22/cloud-computing-sa-industry-update/

Wagner, T.H., and Moshtaf, J., (2016), Individual IT roles in business - IT alignment and IT governance. pp. 4920-4929.Hawaii

Williams., C. (2007) Research Methods. Journal of Business & Economic Research, 5(3), 65-72.

Zhang, Q., Cheng, L., and Boutaba, R.J., (2010), Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications , 1(1), 7–18.

.