Migration of government records from on-premises to cloud computing storage in South Africa

Amos Shibambu[1]
shibaba1@unisa.ac.za ORCID: 0000-0003-3030-0189

Received: 17 March 2022
Accepted: 13 September 2022

The purpose of this study was to investigate the public sector's willingness to entrust their records to cloud computing technology with the view to propose potential strategies to encourage cloud migration. This qualitative study, utilised interviews, and document analysis to collect data. The target population consisted of purposively chosen chief information officers and records practitioners from the national government departments in South Africa. A total of ten participants were interviewed and data were analysed thematically. The study made several findings such as that the government was hesitant to subscribe to the privately-owned cloud due to security concerns such as attack of a physical host, bankruptcy, cross-border jurisdiction, sovereignty, access to information, and data loss, as well as the absence of legislation on cloud storage. The study recommends for the enactment of cloud storage legislation and encourage the storage of digital records on a cloud within the borders of South African virtual space.

Keywords: Cloud storage, records management, digital records, public records, South Africa

1 Introduction and background

There are many definitions of the term "cloud computing" used by researchers, and many more continue to emerge. Laudon and Laudon (2015) define cloud computing (CC) as a model in which computer processing, storage, software, and other services are supplied as a utility over the network, primarily the internet. Al-Mudawi, Beloff and White (2019) describe CC as an application that enables users to access any network from anywhere and share configurable computing resources through easy access to information with minimal management. The National Institute of Standards and Technology (NIST) (2011) comprehensively defines CC as a model for capacitation worldwide, expedient, on-demand network ingress to a communal pool of structural computing resources like servers, services, applications, networks, and storage that can be provisioned expeditiously and emancipated with the least management effort or service provider intercourse.

Since CC is a developing technology, ARMA (2010) claims that it is defined differently by different consumers because it means different things to different communities. This study adopts the definition provided by NIST as it can encapsulate other definitions. The emergence of CC has prompted multitudinous organisations and governments to migrate records to the cloud due to its cost-effectiveness. Usman et al. (2019) suggest that CC proffers opportunities to achieve minimal infrastructure expenses and lower inceptive speculation as compared to a propriety system. It helps to curtail information technology (IT) expenditure without cutting essential services, increase the utilisation of human resources and provide improved services to public servants in their quotidian jobs. Oredo, Njihia and Iraki (2017) and Sabi et al. (2017) agree that the biggest goal of CC is to reduce the cost of IT services while increasing processing throughput, reliability, availability, and flexibility of business operations. Governments can afford cloud computing services as per their requirements. Given its successes, Shen, Yang and Keskin (2012) retrospectively traced the idea of cloud computing back to 1961, when John McCarthy predicted, in a public speech celebrating the Massachusetts Institute of Technology's (MIT) centennial, that computing may someday be organised as a public utility.

Former president of the United States of America, Barak Obama, attests that CC opens the government to its citizens (Paquette, Jaeger & Wilson 2010). Bassett and Schellnack-Kelly (2018) highlight that President Nelson Mandela emphasises the importance of recognising the capacity for people in the 21st century to communicate as a human right. Due to its affordability, Madini et al. (2016) posit that governments and organisations around the world are interested in CC's wealth of growing efficiency and reducing costs. The espousal of CC is informed by its increased trend towards efficient dissemination of digital information. According to Nanos, Misirlis and Manthou (2017), European bodies recommend that countries include CC as an integral part of their electronic government (e-government) services in the view that it promotes government transparency to citizens.

1. Amos Shibambu is Senior Lecturer in the Department of Information Science, University of South Africa

Pederit and Mainoti (2016) observe that CC proves to be a viable model for delivering IT services through the browser. Li, Zhu and Tu (2019) indicate that cloud computing services usually provide online business applications through the browser and a data management centre where software and data can be stored. Stuart and Brommage (2010) point out that, like telephones and electronic mail, browsers have enabled another channel to fulfil business. CC has become a utility, together with the telephone, electricity, gas, and water (Raut, Gardas, Jha & Priyadarshinee 2017). In contrast with the telephone and electronic mail, where communicating parties can identify each other, the widespread coverage of the web means that it is not necessary to know the person who is dealing with the information (Stuart & Brommage 2010; Raut et al 2017). Some of the notable functions of CC used by the public and private sectors include the storage of records and making them accessible without time and geographical constraints. Kriesberg (2017) asserts that the increasingly widespread adoption of computers during the second half of the 20th century changed the ways in which society creates and interacts with information, playing a disruptive role and forcing organisations to adapt or be left behind. Madini et al. (2016) contend that as opposed to on-premises information and communication technology (ICT) storage, cloud consumers do not have control over their data or the performance of the application. In this case, the cloud service provider (CSP) has it.

According to Nanos et al. (2017), CC offers advantages and can be applied to various sectors of the economy, leading to the digital transformation of private and public organisations. Despite the affordability presented by CC to governments and organisations, such as availability, efficiency, cost reduction and high scalability of business operations, it suffers from many deficiencies (El-Gazzar, Henriksen & Wahid 2017). Mohammed, Al-Badi and Mohammed (2016) pinpoint some of the concerns of CC, including a lack of trust in the technology relating to data integrity and security, the absence of an authority that defines policies and sets standards for the adoption of cloud computing in government, and the perception that cloud adoption leads to a reduction in in-house workforce. Despite the good publicity surrounding CC, the global public sector has embraced this service much slower than the private sector (financial and insurance sectors) (Mohammed & Al-Badi 2016). This pace of entrusting records to the cloud is widespread, even in European countries. Not only in South Africa does the adoption of CC hesitate, but the same is also happening in European countries. For instance, Elena and Johnson (2015) mention that despite the publication of the Government Cloud Strategy to promote the adoption of cloud services with the intention of improving the cost-efficiency, flexibility and interoperability of IT services, there is one percent cloud adoption in the public sector of the United Kingdom.

The study's research question was "What are the perspectives impacting the public sector to entrust records in the cloud computing technology?" Emanating from literature results, Elena and Johnson (2015) maintain that there are inadequate efforts to establish what factors influence acceptance or rejection of CC services due to security risk. The objective of this study is to investigate the willingness of the public sector to entrust records to CC technology and to provide potential strategies that would hopefully encourage migration to the cloud.

2 Problem statement

The resultant problem leading to this study was to identify the perspectives influencing the public sector to store records on government premises in South Africa. Government records are accessible to those who can visit the on-premises record storage. This is because government records are securely stored on government premises. As already indicated, Shibambu and Ngoepe (2020) attest that researchers or any person in need of archived records must visit the NARSSA, which is the custodian of government records. According to Shibambu (2020), this storage model comes at a high cost, especially for people who do not live in the vicinity of the archival holdings. However, this is disadvantageous because it is not guaranteed that visiting the premises will yield the required records. This is compounded by the fact that the premises might not be accessible due to an unplanned or planned event such as coronavirus decontamination, revamping, industrial action, and many more hindrances. However, migrating records to the cloud guarantees access to records at any time. Shuijing (2014) postulates that, contrary to the traditional way of record keeping, CC provides data preservation, a high level of expertise on the part of CSP, scalability, affordability, and availability. The author adds that while users are guaranteed access to their data anywhere at any time, CSPs get control over content, set access terms, and monitor usage statistics. Storing records in the cloud would allow easy access to those who are unable to travel to the premises.

3 Purpose and objectives of the study

The purpose of this study was to investigate the public sector's willingness to entrust their records to CC technology and to propose potential strategies to encourage cloud migration. The specific objectives were to:

- determine where the South African public sector stores digital records;
- determine whether the South African public sector trusts cloud storage for records; and

- explore the required terms and conditions for the public sector of South Africa on usage of cloud storage.

4 Literature review

4.1 Storage of digital records

The government is considered the biggest economy in most countries, which should help to set standards and be a potential model provider of user-centric services based on CC technology. Elena and Johnson (2015) posit that adopting CC in the government offers potential benefits such as savings obtained from operating and maintaining hardware and software infrastructures. Mosweu, Luthuli and Mosweu (2019) highlight that CC clients need to appreciate the potential security benefits and threats connected to it and establish realistic expectations with their CSPs. According to Li et al. (2019), CC is aimed at dealing with the existing and looming data-intensive workload. The government of South Africa has a large amount of data that are securely stored on government premises in the form of paper, microfilm, and audio, which is provided in the NARSA Act of 1996. However, the records are not cloud-based, but physically stored in the archival holdings of the government. Usman et al. (2019) postulate that various governments adopt CC due to its increased trend towards efficient dissemination of government services.

It has become inevitable for organisations around the world to adopt the latest technologies such as CC in order to reduce costs, improve efficiency, and deal with the contentious domain (Raut et al. 2017). For example, organisations and some governments have started to reserve virtual space for storage, to which cloud consumers can subscribe. Ning et al. (2015) argue that the purpose of constructing government CC is not necessarily for the government itself, but also to serve the public and public enterprises and to promote the development of the economy and the progress of society. Governments around the world are implementing CC in their quotidian functions to fulfil the purpose of cost curtailment and better utilisation of resources (Usman et al. 2019; Sabi et al. 2015). This motivates the pursuit of greater coherence in the provision of services to the public, public servants, and business partners (Rezza Bazzi, Hassanzadeh & Moeini 2017). However, Abu-Shanab and Estatiya (2017) contend that governments have adopted the latest computing technologies in many countries, but still not enough to consummate the necessities of governments' demands and communal services considering data escalation influences, low efficacy, and obstructions in the alliance. Cloud storage, which is an offering of cloud computing services, provides a wide range of benefits such as efficiency, facilitating the completion of operations and providing high-quality services. Stergiou et al. (2018) point out that cloud computing provides online storage as a framework for the technology.

4.2 Cloud services and deployment models

There is an opinion that the functionality of CC bridges the distance between the government and citizens. Many EU countries have developed a cloud national strategy in line with the recommendations of the European Commission's Cloud Strategy. However, Elena and Johnson (2015) contend that only a few have developed a governmental cloud infrastructure to support their administration. Van Jaarsveldt and Wessels (2015) affirm that governments worldwide are working hard to provide advanced IT-enabled public services to their citizens. In South Africa, the National e-Strategy as contained in the Electronic Communications and Transactions Act (ECTA), No. 25 of 2002, provides that e-government dates back to 1995 when the White Paper on the Transformation of the Public Service was released, but the pace has been very slow. This can be seen in the islands of e-government initiatives in countries where some have been highly successful and are worth replicating. Some of the positive e-government services reflect on the application for smart identity documents. Organisations can afford cloud computing services that they can subscribe to in line with their requirements. Abu-Shannab and Estatiya (2017) add that its billing model of pay-as-you-go charge for utilised services simplifies what the government can migrate to enable virtual access. Al-Mudawi et al. (2019) opine that cloud services contribute to the flexibility of organisational computing, fast deployment, and alignment with IT services, to mention only a few. Shibambu and Ngoepe (2020) hold the view that the public sector does not want to migrate its records to the cloud due to fears relating to data security, privacy, and reliability. Furthermore, the latency, vendor lock, legal issues concerning jurisdiction for data storage and access, contracts, infrastructure providers, conditions of termination, and types of outsourcing are some of the other concerns of CC's espousal. Shibu and Naik (2017) opine that CC and storage solutions provide individuals and organisations with a plethora of capabilities to store and process their data in privately owned or third-party data centres that may be located far from the users. On the other hand, these authors argue that concerns relating to the security of the cloud and privacy hinder various organisations and governments from adopting CC. Given the potential risks associated with CC, Elena and Johnson (2015) indicate that European countries have developed government cloud strategies with the intention of promoting the adoption of cloud services to improve the cost efficiency, flexibility and interoperability of IT services.

Cloud computing comes in the following three types of service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (Reza Bazi, Hassanzadeh & Moeini 2017; Mohammed et al. 2016).

IaaS is the online delivery of virtual infrastructure, which includes servers, storage, and network access (Government of South Australia 2015). This service allows tenants to rent IT rather than procure IT infrastructure on an as-needed basis. The Government of South Australia (2015) also mentions that PaaS is an online delivery of custom application deployment environments in which applications can be built on service provider environments. With this service, customers are enhanced to develop their own software on the platform provided by the service provider. SaaS allows the client to access software that is hosted in the environment of a service provider (Low 2012). Asaeed and Saleh (2015) and the Government of South Australia (2015) suggest that organisations can choose one of the deployment models to deploy their private cloud, community cloud, public cloud or hybrid cloud. Sarkar and Kumar (2016) define a private cloud as one that is dedicated to organisations where computing infrastructure cannot be shared. Considering that the organisation or third party on or off site can manage documents in the cloud, this option is more appealing to organisations that require more control over their data and additional IT infrastructure investment (Sprott 2016). A public cloud is a deployment model that is accessible to anyone and is deemed to be less secure due to its openness (Bhandari, Gupta & Das 2016; Mosweu, Luthuli & Mosweu 2019). Users are expected to register and create user credentials when they use it for the first time. Sarkar & Kumar (2016) state that this infrastructure is hosted at the CSP's premises and there is no way a customer can view the infrastructure. Despite the customer using this deployment model with a low degree of control, Sprott (2016) argues that it still offers enhanced data efficiency and cost-effectiveness.

A hybrid cloud model is an amalgamation of public and private cloud models where some resources are hosted and controlled externally by a third party, while some resources are used only by the organisation (Asaeed & Saleh 2015). According to Bhandari et al. (2016), a hybrid model separates non-critical activities that are performed in the public cloud from critical activities that are performed in the private cloud. Sarkar and Kumar (2016) view a hybrid cloud as a private cloud that can be extended to use resources in public clouds where organisations submit less-valued applications to the public cloud and high-valued applications to the private cloud. These researchers are of the view that this deployment model helps organisations and businesses to take advantage of data hosting and secure applications on a private cloud while still enjoying the cost benefits of keeping applications and shared data in a public cloud. According to Garcia-Galan et al. (2016), it is difficult to select an appropriate configuration for infrastructure, best service, and provider. This can be overcome by fostering a close working relationship between CIOs and records practitioners in order to identify the best cloud storage facility. Some examples of cloud-based storage are Dropbox, Box, Google Drive, and many more, which governments and organisations can use for file sharing (Colicchio, Giovanoli & Gatziu 2015). Given the exorbitant costs of building the infrastructure from the beginning, the cloud models and services are provided by companies such as Microsoft, Google, HP, Amazon, and many other cloud service providers (Colicchio et al. 2015). According to Bezerra and De Mederiros (2013), when governments and organisations lack the capabilities to provide services (IT outsourcing) for strategic reasons, external organisations must step in to fill the void. This IT outsourcing practice is applicable to the storing of records in the cloud. When data are outsourced to cloud storage, the client confers a certain degree of trust on the CSP to take proper security measures in order to protect it from external and internal attacks. This reduces the employees' workload because they have an opportunity to focus their energy on the strategic roles.

Regarding the government perspective, it is worth noting that there are three main target groups that are identified in government concepts, such as government, citizens, and businesses or interest groups. Through CC, e-government operations can be built as cost-effective technology solutions and geographically distributed to heterogeneous resources to improve user service quality. E-government is viewed as an administration system in which governments offer full use of modern technology (Liang et al. 2017). Shibu and Naik (2017) state that e-government is the application of ICT to provide four models of e-governance, namely: government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G), and government-to-employees (G2E), as well as back-office processes and interactions within the entire government framework. Ngoepe (2014) argues that although public servants informally and unconsciously put some records in the cloud, government departments in South Africa are sceptical about entrusting their data to the CSP due to reasons such as the lack of trust in the cloud storage, jurisdiction, legal implications, data privacy and security risk related to the Minimum Information Security Standards (MISS).

4.3 Risks and vulnerabilities associated with cloud computing

Risk is defined as a threat that the use of CC can pose to tasks or situations that might test the abilities of CC by presenting difficulties in allowing for success to be achieved, such as what needs to be overcome to allow CC to prove or justify itself (Bassett & Schellnack-Kelly 2017). According to Elena and Johnson (2015), recent studies have categorised cloud risks into the following four groups: policy and organisational risks (data lock-in, loss of governance), technical risks (cyber-attacks, loss of data), legal risks (data protection and legal jurisdictions) and other risks (network problems, internet connection). Bassett (2015) argues that the risks associated with CC can be greater. To stay relevant to the study, only compliance, as well as legality and audibility, are briefly discussed. Compliance is the awareness of and adherence to

obligations (corporate social responsibility, applicable laws, and ethical guidelines), including the assessment and prioritisation of corrective actions deemed necessary and appropriate. Bassett and Schellnack-Kelly (2018) caution that an organisation that considers utilising an overseas cloud service provider should be aware of the regulatory requirements and legislation pertaining to that specific geographic area. These authors opine that compliance is a significant challenge for CC, both pre-existing compliance and information security standards, which may not be applicable, as they were not originally designed with CC in mind. According to Bassett (2015), legality and audibility relate to an organisation's compliance with operating in accordance with the law and, if inspected, being held accountable. Organisations are expected to comply legally with acts and regulations in their native countries. However, Bassett (2015) argues that with CC, data can reside beyond the borders in diverse geographic locations and jurisdictions, which evokes legal implications requiring considerations such as whether data hosted in foreign countries are subject to the legislation of those countries. CC advantages can be compromised by the hosting laws of other countries and service level agreements of the CSP.

Mohammed and Ali (2016) observe that CC presents a change in managing IT services from owning and managing IT systems to accessing the IT systems as a service when required. Despite the advantages from a business perspective, CC also presents challenges, particularly regarding the distrust of migrating data to an environment over which cloud consumers do not have control. Just like any other organisation, the government departments of South Africa possess various types of data that contain a wide range of sensitivity, which can be catastrophic should they land in the wrong hands. Mohammed and Ali (2016) point out that concerns like security, stability, lack of in-house skills, resources required for migrating applications to the cloud environment, lack of trust in the technology pertaining to data integrity and security, lack of policies and set standards for the adoption of cloud computing in government and diminishing of in-house workforce and data ownership add to the hindrances of cloud espousal. Shuijing (2015) states that risks to data security are compounded by the open nature of CC, and such challenges have prompted scholars to identify and find solutions. According to De Lange, Von Solms and Gerber (2016), the purpose of information security predominantly aims to preserve the confidentiality, integrity, and availability of information. However, many organisations are worried about their users' data being stolen and used for other purposes, which can be associated with breaching of confidentiality. Data security is potentially catastrophic for various types of CC services.

Dahiru, Bass and Allison (2014) assert that security is about the vulnerability of data in the cloud and the fear of attacks by third parties, while privacy is about breach of trust by the CSP of official or personal information. Vulnerabilities are deemed security-related errors that cause weakening or removal of resistance to the environment. Organisational culture, organisational awareness of regulatory compliance, data location, security and privacy are major obstacles towards adopting cloud computing (De Lange et al. 2016). As a result, public confidence in CC is negatively affected. Mohlameane and Ruxwana (2022) indicate that public confidence in relation to cloud computing services fosters doubt and uncertainty pertaining to the safety and privacy of data and the loss of control of data in the cloud environment. In the South African records context, the culture of records management is derived from the NARSA Act of 1996 and is overseen by the NARSSA, which is the state records regulator (Shibambu 2019; Mohlameane & Ruxwana 2022). According to Mohlameane and Ruxwana (2022), other existing legislative frameworks and policies in line with the emergence of cloud computing are the Protection of Personal Information Act (No. 4 of 2013) (POPIA), the Electronic Communication and Transaction Act (No. 25 of 2002) (ECTA), and the South African Competition Act (No.89 of 1998). The POPI Act strives to ensure the privacy, safety, and confidentiality of data subject personal information, that data is processed in a lawful manner, and that there is accountability. It holds the responsible party and the operator accountable for the unlawful processing of personal information.

The ECT Act provides for universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; and to encourage the use of e-government services. The South African Competition Act provides for the establishment of a Competition Commission responsible for the investigation, control and evaluation of restrictive practices, abuses of dominant positions and mergers. The Western Cape Government (2013) adds that the purpose of this Act is to promote and sustain competition in South Africa by ensuring the existence of inclusive participation and the spread of ownership, specifically to previously disadvantaged individuals. If the CSP sells cloud services at a discounted price in order to discourage competitiveness and push competition out of the market, the Act necessitates the intervention by the commission (Mohlameane & Ruxwana 2022). Gonzalez et al. (2017) indicate that the security status of cloud services relies on factors such as security applications running on the system, the hypervisor and associated protection measures, the design patterns used to isolate the control plane from cloud tenants, and protection given by the CSP. The authors also listed the following attacks experienced on cloud computing:

- Outside or inside attack: this exports weakness in cloud access control mechanisms that are on firewalls of the CSP.
- The theft of valid credentials of a cloud user at some location outside the cloud.

- Attacker using valid credentials and prior legitimate access to the cloud.

5 Research methodology

This study took an inductive approach, employing qualitative research methods. As this was a qualitative study, a case study design was used to collect data through semi-structured interviews from ten units of analysis comprised of chief information officers and records practitioners who were purposively selected from national government departments. A case study is an empirical investigation into a current phenomenon set within its real-world context, particularly when the boundaries between phenomenon and context are unclear (Yin 2017). Document analysis was used to supplement data gathered through interviews (policies and procedures on records management). Document analysis is a systematic procedure for reviewing or evaluating printed and electronic (computer-based and internet-transmitted) documents (Bowen 2009). The researcher was able to identify participants based on their quotidian responsibilities in ICT infrastructure and records management thanks to purposive selection.

Records managers, for example, are knowledgeable about records management operations, whereas chief information officers are the departments' technology drivers. The departments included the Departments of Sports, Arts, and Culture, National Archive and Records Services of South Africa, State Information Technology Authority, Department of Basic Education, and Home Affairs. According to Komba and Ngulube (2012), a qualitative study does not necessarily use a larger population, but it still generates significant data for use in the study. Each interview lasted 45 minutes and was aimed at determining the strategies that could be used to develop cloud migration strategies. The units of analysis were anonymised by naming them Participant A through J, as shown in Table 1, and were accessed with permission from their Research and Development Department. Data were analysed using thematic analysis which is the process of discovering patterns or themes in qualitative data (Clarke & Braun 2013). The University of South Africa's Department of Information Science Ethics Review Committee approved this study as ethical (Reference number: 2018-DIS-0006).

6 Discussion of research findings

This section presents discussions and interpretations of the current study in accordance with the study's objective relating to the themes identified during the data analysis process.

Table 1 Participants coding and roles

Participants code	Role
Participant A	Records Practitioner
Participant B	Records Practitioner
Participant C	Chief Information Officer
Participant D	Chief Information Officer
Participant E	Records Practitioner
Participant F	Chief Information Officer
Participant G	Records Practitioner
Participant H	Records Practitioner
Participant I	Records Practitioner
Participant J	Chief Information Officer

6.1 Storage of digital records

The first objective explored the storage of digital records in South Africa's public sector. This study discovered that the government stores digital records on computer devices that are securely kept on the premises under the supervision of NARSSA. Participant B listed external hard drives, flash drives, servers, compact discs, and many other items that are kept in a secure room as the heart of digital storage. The government appears to be content with on-premises storage because it has complete control over the records. Participant B expressed concern about rapid technological changes that could render records or devices obsolete. This participant elaborated that they used the dictabelt, which were converted into external hard drives when there were no devices to retrieve the data stored on them.

During the interview, while acknowledging that the records are kept on site, Participant A stated that the government is planning to migrate to the cloud. "There is a specific architecture, and we are moving to the cloud," says Participant A. Participant A added: “I can respond to that, government cloud. The old niche was housed by SITA in Centurion, and the

new one, INSENSE OF ATOM, will be housed at SITA Centurion as well, but on the government cloud." At the same time, due to security concerns, this participant was hesitant to have records migrated to privately owned cloud. "We cannot afford for our records to be kept by institutions in India because it is government information. We cannot let the private sector control our data, which is why we are not moving to the government cloud. We want the government cloud to be in SITA and under SITA control," said Participant A. Participants agreed that the government cloud is solely the responsibility of SITA, which has been mandated by the state to manage the state's IT services. Participant I, for example, pointed out that digital records are stored on SITA's servers. This participant agreed that SITA, along with DAC-IT, is responsible for storing records for the time being. This was confirmed by Participant J, who stated that the national archives are kept at SITA, whereas other records are kept on-premises servers.

Even though the records are stored locally on the digital devices, it was confirmed that SITA already had cloud storage, which is referred to as a government cloud. Furthermore, other government agencies are purchasing cloud storage from the government cloud. According to Participant C, on-premises storage will be phased out in favour of cloud storage. "We are migrating to the cloud. We are implementing SharePoint, which will be hosted on a cloud server. Now, they are on physical servers, but in a few months, they will only be in the cloud. We plan to return everything to the cloud within five months. We will be migrating everything there shortly after that. We will manage the cloud internally, as well as the space purchased by each government department. For the time being, we have five departments, including DAF, the Limpopo Premier's Office, DST, SITA, and DAC. The records will be moved to the cloud, but it will be a project. It is a process that we must implement in order to move to the cloud."

Participant D admitted that the government stored records manually. The participant went on to explain that the records on the servers were not structured in accordance with the file plan. "We have not yet reached that level. We only do manual storage in accordance with the file plan." Participant F confirmed, in support of Participant D, that the digitally stored records did not adhere to proper information governance and that there is no relationship between records management and IT sections. "There is no proper information governance in this department to say who accesses which information, how do we categorise information," Participant D demonstrated, adding that "we just throw anything at it; digital photos are on the networked drive. There is no organised method of storing data, records, or digital records. The structural and cultural arrangements contribute to the silo mentality, such that records management is doing their own thing and records management is duplicated, for example, records management in registry, records management in HR, and other locations within the department." There was duplication, according to this participant, because there was no proper structure that spoke to all the records in the department. Others were assigned to work with records in this case, and they only uploaded what they had. Before digital storage can be formalised, according to Participant E, training on the use of digital storage and digital records is required.

Participant G revealed that a private company was tasked with digitally storing government records outside of government premises. Given the nature of silo operations in the public sector, this private company collaborated with a records management section where the role of the government records practitioners was to scan the records and upload them to the private sector's system. This participant was concerned about the company in charge of the state's digital records. Furthermore, the participant painted the following picture: "I do not know what will happen to the records when it collapses or liquidates. Keep in mind that all HRM sections use the same system. They scan the original copy before bringing it to the records section. The service provider handles most of the functions, and I am not sure if the department will ever need to transfer skills. The chief director proposed it, but the private sector expects money for every task completed. We want that information. Currently, the service provider provides IT support. We put in a call, and they come out to fix it. Contracts for IT support and digital records management have been awarded to the department." This discovery confirms the department's functional silo operations, which had extended to IT functions even though the department had an IT section that provided IT support services.

The researcher discovered boxes of files all over the floor during her visit to the site for the scheduled interview. "We are running out of space to keep hard copies, which is why you see boxes lying around. We will send them to offsite storage...even if it is a private company, we can account for them," Participant G explained.

6.2 Entrusting records in the cloud

The second objective was intended to find out if the public sector entrusts records to the cloud. It emerged that the government does not trust cloud storage. According to Participant A, "the whole database is going to the cloud. The government cloud... SITA Centurion, … We do not want outside companies to manage our data." This was a glaring response that they did not trust the privately owned cloud storage. This study revealed that the migration to the cloud was necessary, but only to the government-owned cloud. According to the participants, a privately owned cloud carries security risks, and that makes the government more sceptical of cloud storage. Participant B postulated, "We are very conscious of who owns the cloud. What if the owner of the cloud is an enemy of the superpowers who can bomb the country and the

cloud during the war? The private companies owning the cloud can go bankrupt. We have less trust in the third party. When Cabinet memos land in the wrong hands, there's trouble." Participant D demonstrated that, "personally, yes, if the security aspect is strengthened. It is not a question of trust; it is a question of how we are regulated to interact with SITA. The SITA ACT stipulates that it is compulsory for all government departments to do business with SITA." According to Participant E, records can be entrusted to the cloud, but it must be a government cloud. The participant mentioned that only if it failed, would the private cloud receive recognition. Although the determination of the NARSA Act has been highlighted as an ethical compass that guides the consideration of the cloud, this study established that government departments subscribe to privately owned clouds to host services such as online exchange for email services. According to Participant F, "Now we have a contract with IS, who subcontracted Mimecast, where emails from this department are stored on the Mimecast cloud. That means we entrust our records to the cloud." Some participants were oblivious to online storage services. "I can't say yes or no, because I don't know how they reached their agreement. I only comply. I was given a system to use, and they trusted them. I do not trust people to handle my personal information. The department trusts the service provider, and I comply. (Yes, I am not sure of the model, but I understand the government cannot work with a service provider that is not legal or appointed by the HoD (text)", Participant G mentioned.

Despite not being aware of what is happening in the government regarding cloud storage, some senior records practitioners are completely uninterested in the storage of records. Participant H had no idea whether or not to trust records in the cloud. According to this participant, "The records management section is just within the directorate, but I'm less interested in it." Another seasoned participating records practitioner (Participant I) believed that cloud storage was beginning to lose the ante. According to this participant, "I've been to a few conferences in Europe for a few years dealing with archival matters. Many institutions around the world are moving away from the cloud for various reasons: (1) costs (they believe it is less expensive to build an in-house capability), (2) some archival repositories (your records can be held hostage when you use a private cloud, for example, you agree to pay R1 p/m, but the organisation changes to R2 p/m, which you did not agree to), and if you refuse to pay, they keep information, (3) Bankruptcy: a private company may go bankrupt and disappear with your information, and (4) foreign governments may gain access to your information. Some governments' legislation forces other governments to make the information available. Then it is not safe and secure. But if it is a government cloud held by SITA, our records will not be held hostage. Therefore, I do not trust private clouds." On the other hand, there is a need to entrust records to the cloud, but there are obstructions. "Yes.

The hindrances to cloud computing were sovereignty and cross-border jurisdiction. If the cloud is in Russia, for example, we do not even know where the physical storage is. To circumvent that, government records must be in the government-owned cloud. I won't have any problems if it is owned by the government. When I go to the privately owned cloud and that company goes under, I stand a chance of losing data that is in their possession. If the company survives and there is a legal dispute, the USA's laws will apply, not South Africa's. The courts of the USA will have jurisdiction over the matter, not South African law. But if it is within our borders, we will not have such issues. If we have disputes, the company will give back the records, of course at a high cost. Accepting the records back might be an issue because I do not have the equivalent storage capacity. However, what assurance do we have to prove that they don't have a copy? And I would prefer the hybrid cloud. Creating our own cloud is costly," Participant J explained.

6.3 Terms and conditions for cloud storage

This objective intended to establish the terms and conditions that the public sector of South Africa might require when migrating to the cloud. The researcher also probed what terms and conditions should be used when migrating records to the cloud. Because cloud computing is new in the public sector of South Africa, the participants told the researcher that migration to the cloud should comply with terms and conditions for storage of records determined by the government. For instance, Participant B suggested that the government be in control of the cloud, perform the DRP, provide full access to records managers, and that the cloud must be within the borders of South Africa. The government legislated the NARSA Act of 1996, which provides how records and archives should be managed. Participant D indicated that all the regulations and standards in terms of reference must be drawn from the existing archiving Act. However, the findings of this study revealed that some government departments have entered contractual obligations for archival holdings with the private sector.

In this regard, Participant G indicated some oblivion in terms and conditions of the storage the government has with the private sector. Participant G further indicted that, "I do not know what is happening to the records after scanning. I do not even know how many people the service provider has access to. Internally, every record practitioner has access to the digital records." Participant I emphasised the importance of records practitioners having full access to the records. Participant I went further to explain, "My organisation will always have access to all the information that it stores. No information may be given to the third party. Information should always be available. There should be sufficient security to ensure that information is not hacked, changed, deleted... People working with information should have security clearance."

It is widely believed that state records remain the property of the government. This is based on Participant J's view that "intellectual property of the government remains property of the government. Any record we take there remains the record of the government. Assurance on issues of security and cyber security measures to protect whatever we put in the cloud."

7 Conclusion and recommendations

The problem of perpetual manual record storage on the premises of South Africa's public sector prompted this study. The purpose of this study was to investigate the migration of South African government records from on-premises to CC storage. The public sector generates a wealth of data that is useful to both civil servants and citizens. It was determined that digital records are stored on computer devices that may become obsolete and impossible to retrieve or access as a result of technological changes. This is the situation that the government faced during the dictabelt era, when the technology became obsolete, forcing the government to find other ways to retrieve data. Information is the lifeblood of any organisation, and it leaves a trail that cannot be erased. Another reason for on-premises storage was that the government was hesitant to subscribe to the privately owned cloud due to security concerns such as physical host attack, bankruptcy, cross-border jurisdiction, sovereignty, access to information, and data loss. Even though the cloud has become a popular model for records storage with the benefit of easy access regardless of geographical zone or time, the government does not entrust records to the cloud. Terms and conditions must be developed if the government entrusts records to the cloud. In this regard, this study makes the following recommendations:

- The government must take bold steps to review current physical storage and develop a government cloud (G Cloud) within South African borders, inviting government departments to subscribe to the storage.
- Given that cloud storage is still relatively new in the public sector, all records practitioners must be trained. In view of the large number of government records, the development of a records migration strategy committee to the cloud to improve ubiquitous accessibility of records should guide record prioritisation. In the absence of cloud service provisioning capabilities, the private sector must be enlisted to fill the IT sourcing gap. Because cloud storage is already available in the private sector, the government should consider public-private partnerships to reduce the start-up costs of developing a cloud. However, if this option is chosen, policies and role definitions must be clearly defined.
- To develop a record migration strategy to the cloud, the government must form a committee led by the Department of Sport, Arts and Culture. This committee must determine the level of clearance conditions that must be applied to digital records.
- To ensure that records are in good hands, all records practitioners must have security clearance.
- The government must reduce silos and establish an integrated records management section, even if this necessitates the creation of several subsections.
- The government must promote cloud storage awareness through the Arts and Culture Department.
- The government must upskill the current workforce so that they can easily adjust to the new working environment.
- To mitigate the risks associated with the cyber environment, a cyber-security team must be formed.

References

Abu-Shanab, E and Estatiya, F. 2017. Utilizing cloud computing in public sector cases from the world*. International Conference on Applied System Innovation (ICASI)*. 1702-1705.

Al-Mudawi, N, Beloff, N and White, M. 2019. Cloud computing in government organisations: towards a new comprehensive model. *SmartWorld, Ubiquitous intelligence & computing, Advanced & Trusted computing, scalable computing & communications, Cloud & Big Data computing, internet of people and smart city innovation*. 1473-1479.

ARMA International. 2010. Making a jump to the cloud? How to manage information governance challenges. [Online]. https://www.arma.org/docs/hot-topic/makingthejump.pdf (12 January 2022).

Asaeed, N. and Saleh, M. 2015. Towards cloud computing services for higher educational institutions: concepts and literature review. *Cloud computing, International Conference on Cloud Computing, Riyadh, Saudi Arabia, 26-29 Apri*l.

Bassett, C. 2015. *Cloud computing and innovations: its viability, benefits, challenges and records management capabilities*. Master's dissertation. University of South Africa, Pretoria.

Bassett, C and Schellnack-Kelly. 2018. Risks associated with cloud computing in pursuit of effective records management*. ESARBICA Journal: Journal of the Eastern and Southern Africa Regional Branch of the International Council on Archives*. 37:89-110

Bezerra, T.R. and De Mederiros V.L.C. 2013. Managing customers' IT capabilities in IT outsourcing over time: A system dynamic approach. *IFIP/IEEE International Symposium on Integrated Network Management* (IM 2013).

Bhandari, A., Gupta, A. and Das, D. 2016. A framework for data security and storage in cloud computing. *International Conference on Computational Techniques in Information and Communication Technology, New Delhi*, India, 11-13 March.

Bowen, G.A. 2009. *Document analysis as a qualitative research method*. North Carolina: Western Carolina University.

Clarke, V. and Braun, V. 2013. *Thematic analysis. In: AC. Michalos (Ed.) Encyclopaedia of quality of life research*. New York: Springer.

Colicchio, C., Giovanoli, C. and Gatziu, G.S. 2015. A cloud readiness assessment framework: for enterprise content management and social software (e-collaboration) in small and medium sized enterprises. Paper read at 3rd *International Conference on Enterprise System*, Basel, Switzerland, 14-15 October.

Dahiru, A.A., Bass, J. and Allison, I. 2014. Cloud computing: Adoption issues for sub-Saharan Africa SMEs. *The Electronic Journal of Information Systems in Developing Countries* 62(1): 1-17.

De, S.J. and Pal, A.K. 2017. A policy-based security framework for storage and computation on enterprise data in the cloud. *47th Hawaii international conference on system sciences Waikoloa, HI, USA*, 6-9 January.

De Lange, J., Von Solms, R. and Gerber, M. 2016. Information security management in local government. In Cunningham, P & Cunningham, M. (eds). 2016. *IST-Africa Week Conference, Durban, South Africa, 11-13 May*. [Online]. http://www.ist-africa.org/conference2016 (13 January 2021).

Elena, G. and Johnson, C.W. 2015. Factors influencing risk acceptance of cloud computing services in the UK government. *International Journal on Cloud Computing: Services and Architecture*, 5:2

El-Gazzar, R., Henriksen, H. and Wahid, F. 2017. IT innovation and entrepreneurship in emerging economies – Is cloud computing a magic ingredient for Egyptian entrepreneurs? *In proceedings of the 25th ECIS, Guimaraes, Portugal*, June 5-10, 1044-1061.

Garcia-Galan, J., Trinidad, P., Rana, O.F. and Ruiz-Cortes, A. 2016. Automated configuration support for infrastructure migration to the cloud. *Computer Systems*, 55: 200-212.

Hamid Reza, B, Hassanzadeh, A. and Moeini, A. 2017. A comprehensive framework for cloud computing migration using Meta-synthesis approach, *Journal of Systems and Software*, 128 (87-105).

Gonzales, D., Kaplan, J.M., Saltzman, E., Winkelman, Z. and Woods, D. 2017, Cloud-trust – a security assessment model for infrastructure as a service (IaaS) Clouds. *Transactions on Cloud Computing*, 5(3).

Government of South Australia. 2015. Cloud computing and records management. [Online]. https://governemnt.archives.sa.gov.au/sites/default/files/20150706%/2cloud%20computing%20and%20Records%20Management%20Final%20v1.pdf (17 January 2022).

Komba, M.M. and Ngulube, P. 2012. E-government adoption in developing countries: trends in the use of models. *ESARBICA Journal*, 30(1): 162-176.

Kriesberg, A. 2017. The future of access to public records? Public-private partnership in United States and territorial archives. *Archival Science*, 17:5.

Laudon, K.C. and Laudon, J.P. 2015. *Management Information Systems: Managing the Digital Firm Plus MyMISLab with Pearson eText*. 14th ed. New Jersey: Prentice Hall Press.

Li, Y.L., Zhu, L. & Tu, W. 2019. "Research on e-government data management in cloud computing environment*". 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), Xiangtan, China*, 289-292.

Liang, Y., Qi, G., Wei, K. and Chen, J. 2017. Exploring the determinant and influence mechanism of e-Government cloud adoption in government agencies in China. *Government Information Quarterly*, 34:481-489.

Low, H.A. 2012. Primer on policy implications of cloud computing. [Online]. http://ftp.maps.canada.ca/pub.nrcan_rncan/publications/ess_sst/291/291945/cgdi_ip_20e.pdf (10 January 2022).

Madini, O.A., Alharthi, A., Walters, R.J. and Wills G.B. 2016. Security risk factors that influence cloud computing adopting in Saudi Arabia government agencies. *International e-Conference on Information Society (i-Society 2016)*.

Mohammed, F., Ibrahim, O. and Ithnin, N. 2016. Factors influencing cloud-computing adoption for e-government implementation in developing countries: instrument development. *Journal of Systems and Information Technology*, 18(3): 297-327.

Mohammed; A. and Mohammed, Z. 2016. Review on hybrid extreme learning machine and genetic algorithm to work as intrusion detection system in cloud computing. *Journal of Engineering and applied Sciences*, 11(1): 460-464

Mohlameane, M. and Ruxwana, N. 2020. Exploring the impact of cloud computing on existing South African regulatory frameworks. *South African Journal of Information Management* 22(1), a1132.

Mosweu, T, Luthuli, L. and Mosweu, O. 2019. Implications of cloud-computing services in records management in Africa: Achilles heels of the digital era? South African Journal of Information Management 21(1), a1069.

Nanos, I., Misirlis, N. and Manthou, V. 2017. Operational research in the digital era – ICT challenges*. 6th International Symposium and 28th National Conference on Operational Research*, Thessaloniki, Greece, June 2017.

National Archives and Records Service of South Africa. 2007. Records management policy manual. Pretoria: NARS. [Online]. http://www.national.archives.gov.za/rms/Records_Policy_Manual_October_2007.pdf (12 December 2020).

Ngoepe, M. 2014. The role of records management as a tool to identify risks in the public sector in South Africa. *South African Journal of Information Management,* 16(1): Art. #615, 8.

Ngoepe, M. 2017. Archival orthodoxy of post-custodial realities for digital records in South Africa. *Archives and Manuscripts* 45(1): 31-44.

Ning, W., Xiaoshan, X., Hui, L. and Xuehua, W. 2015. Survey of application and research on government cloud computing in China. 2015 *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology. Singapore* 140-143.

Oredo, J., Njihia, J. and Iraki, X.N. 2017. The role of organizing vision in cloud computing adoption by organizations in Kenya. *American Journal of Information Systems,* 5(1): 38-50.

Paquette, S., Jaeger, P.T. and Wilson, S.C. 2010. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 27: 245-253.

Pederit, R. and Mainoti, G. 2016. Mitigating user concerns to maximize trust on cloud platforms. 1st-Africa Durban, South Africa, 13-15 May 2016 conference. [Online] https://www.ufh.ac.za/faculties/commerce/departments/information-systems/publications/mitigating-user-concerns-maximize-trust-cloud-platforms (18 December 2021).

Raut, R.D, Gardas, B.B, Jha, M.K. and Priyadarshinee, P. 2017. Examining the critical success factors of cloud computing adoption in the MSMEs by using ISM model. *International Journal of Computers in Human Behaviour*, 76: 341-141.

Rezza Bazi, H., Hassanzadeh, A. and Moeini, A. 2017. A comprehensive framework for cloud computing migration using Meta-synthesis approach". *The Journal of Systems and Software*, (128): 87-105.

Sabi, H., Uzoka, F.M.E., Langmia, K. and Njeh, F.N. 2015. Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management,* 36(2):183-191.

Sabi, H.M., Uzoka, F.M.E., Langmia, K., Njeh., F.N. and Tsuma, C.K. 2017. A cross-country model of contextual factors impacting cloud computing adoption at universities in sub-Saharan Africa. *Information Systems Frontiers*, 20: 1381-1404.

Sarkar, M. and Kumar, S. 2016. *A framework to ensure data storage security in cloud computing. IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*. New York: United States of America.

Saunders, M., Lewis, P., Thornhill, A. and Bristow, A. 2019. *Research methods for business students*.12th ed. Harlow, UK: Person Publishers.

Shen, Y., Yang, J. and Keskin, T. 2012. The evolution of IT towards cloud computing in China and US. *International Conference on Computational Problem-Solving, Leshan, (China)*, 19-21 October.

Shibambu, A. and Ngoepe, M. 2020. When rain clouds gather: Digital curation of South African public records in the cloud". *South African Journal of Information Management*, 22(1): 205.

Shibambu, B.A. 2019. *Digital curation of records in the cloud to support e-government services in South Africa*. PhD Thesis. Pretoria: University of South Africa.

Shibu, S. and Naik, A. 2017. An approach to increase the awareness of e-governance initiatives based on cloud computing, *International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, Indore, 1-4.

Shuijing, H. 2014. Data security: the challenges of cloud computing. *Sixth International Conference on Measuring Technology and Mechatronics Automation*. Shanghai, China, 10-11 January.

Sprott, A.A. 2012. Let me in the cloud analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime*, 20(1): 6-24.

Stergiou, C., Psannis, K.E., Kim, B.G. and Gupta, B. 2018. Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, 78: 964-975.

Stuart, K. and Bromage, D. 2010. Current state of play: records management and the cloud. *Records Management Journal*, (20):217-225.

Usman, A., Hafiz, A.U., Ammar, S. and Zain, U.I.A. 2019. Government cloud adoption and architecture. *ICCMET*, China.

Van Jaarsveldt, L.C. and Wessels, J.S. 2015. Information technology competence in undergraduate public administration curricula at South African universities. *International Review of Administrative Sciences*, 1-18.

Western Cape Government. 2013. The Competition Act 89 of 1998. [Online] https://www.westerncape.gov.za/legislation/competition-act-89-1998 (15 February 2022).

Yin, R.K. 2017. *Application of case study research*. London: Sage.