South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

When rain clouds gather: Digital curation of South African public records in the cloud

Authors:
Amos Shibambu[1]
Mpho Ngoepe[1]

Affiliation:
[1]Department of Information Science, Faculty of Arts, University of South Africa, Pretoria, South Africa

Corresponding author:
Mpho Ngoepe,
ngoepms@unisa.ac.za

Dates:
Received: 13 Feb. 2020
Accepted: 16 July 2020
Published: 07 Oct. 2020

How to cite this article:
Shibambu, A. & 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), a1205. https://doi.org/10.4102/sajim.v22i1.1205

Background: Many scholars lament of poor infrastructure for the management and preservation of digital records in the public sector in South Africa. For example, in South Africa, the national archives repository and its subsidiary provincial archives do not have infrastructure to ingest digital records into archival custody. As a result, digital records are left to the creating agencies to manage and preserve. The problem is compounded by the fact that very few public sector organisations in South Africa have procured systems to manage digital records.

Objective: This study investigated whether government departments in South Africa entrust their records to cloud storage. The study asked the questions: How are digital records managed and stored in these organisations? Do government departments entrust their records to the cloud as an alternative storage?

Method: Qualitative data were collected through interviews with purposively chosen chief information officers, records managers and IT managers from public entities that implemented e-government services, as well as officials from the National Archives and Services of South Africa, which is charged with the statutory regulatory role of records management in governmental bodies and the State Information Technology Agency, a public sector Information Communication Technology (ICT) company established in 1999 to consolidate and coordinate the state's information technology resources.

Results: The key findings suggest that although public servants informally and unconsciously save some records in the cloud, government departments in South Africa are sceptical to entrust their records in the cloud because of a number of reasons such as lack of trust in the cloud storage, jurisdiction, legal implications, privacy and security risks related to Minimum Information Security Standards, as well as lack of policy and legislative framework, specifically regarding cloud storage.

Conclusion: Because of lack of infrastructure for management and preservation of digital records, for the purpose of increased storage and access, this study recommends that government departments should cautiously consider exploring the possibility of storing their records in a trusted digital repository cloud as an interim solution whilst observing legal obligations. As cloud storage is not very prevalent amongst government departments in South Africa, given the present challenges in managing digital records, it would be advantageous to have cloud storage tested rigorously before embarking on the exercise.

Keywords: digital curation; cloud storage; public records; e-government; South Africa.

Introduction and background to the problem

The title of this article was inspired by the classical novel by Bessie Head (2013) titled *When rain clouds gather*. The story of the novel is set in a fictional village in a remote area on the eastern side of Botswana. The country, or even so the fictional village, is dominated by the Kalahari Desert and the land is barren because of below average rainfall, often accompanied by severe drought. In her novel, Bessie Head uses the nation's constant desire for water as a backdrop for the hopes and aspirations of the people she describes. Despite the harshness of the land, people constantly look with hopefulness for rain clouds. This scenario can apply to the situation of records storage in the cloud in South Africa.

In South Africa, the responsibility of regulating government records falls under the auspices of the National Archives and Records Services (NARSSA) in the Department of Arts and Culture (DAC), which according to Ngoepe (2017) does not have the necessary infrastructure to manage and preserve digital records. As a result, digital records are left to the creating agencies to manage and preserve. The problem is compounded by a lack of government policy or legislation that regulates the storage and digital curation of records in the cloud. As a result, policies that regulate the storage of records in the cloud do not exist, which leaves government departments to put away paper-based records in an inaccessible storage with only few authorised users to access such records (Higgins 2011). This leaves government departments to face challenges like limited access to data in the provision of improved service delivery, as well as a lack of storage space for both paper and digital records. The alternative for this could be cloud storage. Neelima and Padma (2014) defined cloud storage as a storage medium that maintains data, manage and backup remotely and makes data available to users over the network or internet. Cloud storage has become an increasingly viable storage option for organisations that are unable to afford or maintain in-house, private electronic infrastructure suitable for long-term preservation of digital holdings. A reliable cloud archive that meets the requirements and expectations of a trustworthy repository is still in the early stages of conception.

The significance of cloud storage to e-government is well documented, and it improves ways of providing services to the citizens of a country. For example, Paquette, Jaeger and Wilson (2010) indicated that former president of the United States of America, Barak Obama, is of the view that cloud computing is capable of opening up the government to its citizens. The contribution of cloud storage to e-government services has the potential to merge distance and space and reduce time, which makes the transactions of public service more effective. For example, a citizen can apply for identity document or passport online without visiting the concerned government department or a potential tourist of the country can apply for a visa online without visiting the embassy. Following their impressive work, Shen, Yang and Keskin (2012) traced the conception of cloud computing back to 1961 when John McCarthy, whilst giving a speech to publicly celebrate the Massachusetts Institute of Technology's (MIT) centennial, that computation may someday be organised as a public utility. Just like electricity and telephones, subscribers will need to pay for the capacity of the usage of the space they acquired from the cloud service providers (CSPs). The situation leads to more storage for digital records on the cloud.

In the context of public administration, storing records in the cloud seems to be a cost-effective means of delivering e-government services towards ensuring efficiency, effectiveness, transparency, interoperability, cooperation, sharing and security. Bouaziz (2008:12) mentioned that the popular roles of e-government services are to allow collaboration of the government and its citizens (G2C) and to enable inter-agency relationships (G2G). However, that is achievable in the presence of cloud computing and digital preservation, which enable retrieval of records in various places at the same time. Carter and Bélanger (2005:5) observed that one of the primary functions of e-government is to ensure accessibility of government services to citizens and to promote a cost-effective government. Its success is solely reliant on a platform of cloud storage. In all organisations, data ostensibly have a strategic tool that is needed to support e-government. Given that the South African government envisions the offerings of government services through e-government services and has already partially realised the vision (application of identity documents, passport online, as well as filing of tax returns), it is necessary to have digital preservation in the cloud in order to support such services (Katuu & Ngoepe 2015).

Whilst the findings of iResearch of 2012 indicated that cloud storage service is already technically matured, its promotion is still in its infancy and that can be ostensibly seen in the way record keeping is handled. South African government departments have their records in their registries where they are accessed manually because they are stored predominantly in the form of paper, audio-visual and microfilm (Ngoepe 2012). Notwithstanding the importance of cloud storage, the challenge with the current practice in the context of the South African government still remains as records are stored on the premises of each department's registries manned by untrained registry clerks. Only a few governmental bodies have automated their records management programme (Ngoepe 2017). Pickover and Harris (2001) maintained that traditional paper-based records are likely to be inefficiently provided with resources, manned by junior records practitioners with little status and subject to high turnover rates, and incorrectly connected, if at all, to a parallel or similar electronic records management system. Rightly so, cloud storage is not prevalent amongst government departments in South Africa. Kuiper et al. (2014:1) opined that despite the potential advantages offered by cloud computing such as cost reduction in setting up cloud storage infrastructure, increased flexibility and agility when sharing archived records, the public sector in South Africa lags behind.

Problem statement

Despite a myriad of potential opportunities officered by the cloud storage, the current practice suggests that the South African government stores archival records on the government premises. This is informed by the *NARSSA Act of 1996*, which does not promote the use of cloud in favour of local digital storage, for example, external hard drives, compact discs, to mention but a few that are securely locked on the premises. However, on-site storage hinders ubiquitous access of records. Kuiper et al. (2014) pointed out that such practice does not promote the rollout of e-government service that is envisioned by the South African government. Obrustky (2016) and Galloway (2013) suggested that one key advantage of cloud storage is that the organisations can access information from any location, even if they do not have access to their organisation's network. This view is confirmed by Rajan and Shanmugapriyaa (2012) who stated that the strategies of cloud storage are capable of transforming the way in which current organisation's infrastructure is constituted and managed. Whilst providing easy access of records from anywhere, such strategies can save the organisations' capital expenditure and focus on operational expenditure. Given the evolution of technology, the use of cloud storage can save the organisation from the obsolescence of either the storage devices or stored information. In that view, there is a need for the South African government to review its physical storage model of records in favour of cloud in order to improve accessibility that is not limited by time and location.

Purpose and objectives of the study

The purpose of this study was to explore digital curation of records in the cloud to support e-government services in South Africa. The specific objectives were to:

- analyse policies and legislative framework for records storage in the cloud;
- determine if the public sector entrusts records in the cloud for storage and preservation; and
- suggest a framework for digital curation of records in the cloud.

Literature review

Literature for this study is focused on the types of cloud storage, policy and legislative framework, storage and digital preservation of records in the cloud.

Cloud storage and preservation

Since its introduction, the cloud has become one of the fastest growing business for the storage of data. It involves storing data with cloud service provider rather than on local systems such as external hard-drive, compact disc, to mention but a few. Galloway (2013) pointed out that with the use of cloud storage consumers can access data from any location even if they do not have access to the network of an organisation.

Some organisations are now relying on the cloud for their record-keeping and preservation needs (Leveille 2015). It is indeed a viable storage option for organisations that are unable to afford or maintain in-house storage and preservation infrastructure. Instead of the traditional in-house records storage infrastructure, records are hosted virtually by the cloud service provider. In the past, storage of records has been an in-house activity. This, according to Cunningham (2019), offers the greatest degree of control and maximum opportunity for aligning to local policies. On the other hand, contracting, especially with CSPs, can provide organisations with access to the richest technical resources. However, this entails the risk of loss of control and knowledge of how preservation is carried out. This is compounded by the fact that cloud services may also run afoul of legal requirements regarding data residency, data protection, privacy and intellectual property rights (Cunningham 2019).

It is common for public sector organisations to encourage the use of cloud services. Cunningham (2019) recommended that when considering cloud storage, users should take into consideration the governance of data as it is the key factor in ensuring the security of information; compliance, especially with regard to the jurisdiction of the cloud service provider; trust; architecture; access management and software isolation; incident response and availability in case a court orders a seizure of equipment.

According to Pearce-Moses (2019), cloud storage is the storing, processing and use of data on remotely located computers accessed over the internet. Given the nature of its design, data in the cloud storage cannot be accessed in the absence of network connection. Bazi, Hassanzadeh and Moeini (2017) identified three types of service models: software as a server (SaaS): (1) a model where software and other solutions are delivered to the end-users as a service using the internet rather than as a product that can be installed on users' computers or mobile devices (Park & Ryoo 2012:161); (2) platform as a service (PaaS): an extension of SaaS that provides a platform to build and run application packages using an Application Programming Interface (API) that is supported by CSP; and (3) infrastructure as a service (IaaS), which is hosted by CSPs. All of these are accessed using the internet as a principal communication channel. Bazi et al. (2017) suggested that this pay-as-you-go platform allows an organisation to outsource its entire IT infrastructure to a CSP in support of its day-to-day operations such as servers, software, technical support and storage. It allows users to control or manage computing resources such as storage, networks and computing power so that they can deploy and run arbitrary software.

Each of the above service models can be deployed onto one of four variables types of clouds identified as follows:

- Public cloud model: It is a deployment model that is accessible to anyone and is deemed to be less secure because of its openness (Bhandari, Gupta & Das 2016). Some examples of public cloud are Microsoft Azure, Google Cloud and Amazon. It should be noted that the term 'public' does not always associate with 'free', despite being fairly cheap.
- Private cloud model: It is dedicated to organisations where the computing infrastructure cannot be shared (Leveille 2015). Considering that the organisation or third party on site or off site can manage it, it is more appealing to the organisations that require more control over their data and additional IT infrastructure investment (Sprott 2012).
- Hybrid cloud: This model is an amalgamation of public and private cloud models where some resources are hosted and controlled externally by a third party, whilst some resources are used only by the organisation (Sprott 2012).
- Community cloud model: This is a deployment model shared by organisations of the same community (Leveille 2015) that have shared concerns, for example, mission, security requirements, or compliance considerations. Bhandari et al. (2016) argued that community cloud is not really a deployment model as it is like private cloud, with the difference that in this case systems and services are accessible by a group of organisations.

Digital curation encompasses the processes and controls that enable digital objects to survive over time. The challenges for digital curation of records include both intentional and accidental corruption and loss throughout their existence. This requires that the records, even if entrusted to the cloud, are controlled under an unbroken chain of preservation (Duranti 2005). McLeod (2019) identified three strategies for preserving records in the cloud as involving the service provider to assume preservation responsibility, building a framework for preservation and access that can be implemented through a series of interconnected but independent services and, lastly, harnessing the emerging blockchain technology.

Policy and legislative framework

This section reviews literature from a legislative and regulatory framework perspective and explores some of the fundamental issues in managing records in a digital environment where cloud computing is gaining prominence. In the face of all these developments, the challenge is whether the legislative and regulatory framework in South Africa is adequate to facilitate the management of digital records in public institutions. Digital records are a reality for all public sector institutions, both in the national government and in other public sector institutions. In South Africa's myriad laws and regulations relating to the management of public records, electronic communications, privacy and data security are largely based on the principle of territoriality (Katuu 2015). A key concern is the loss of jurisdictional control over public records that may be managed and stored in disparate locations, including outside the country. Katuu (2015) identified three legislative instruments that 'control information' across all public institutions as: the archival legislation, which is *NARSSA Act*; the freedom of information legislation, which is the *Promotion of Access to Information Act*; and the privacy legislation, which is the *Protection of Personal Information Act*. The *NARSSA Act* imbues the national archivist with the power to determine the conditions of properly managing and reproducing electronic records.

Ngoepe and Saurombe (2016) pointed out that the legislation contains an important function, particularly on how records are stored in a networked environment in any country. In order to facilitate the management of digital information there are several additional legislative instruments, two of which are the *Electronic Communications and Transactions* (*ECT*) *Act* that was promulgated in 2002 and that facilitates ECT and the *Regulation of Interception of Communications Act* (*RICA*) that was promulgated in 2002 and regulates the interception of certain telephonic as well as internet communication. The *NARSSA Act* provides that governmental bodies are required to put the necessary infrastructure, policies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner. However, in reality, this is not the case because, according to Ngoepe (2012), records management programmes in governmental bodies in South Africa are on the brink of collapse because of lack of infrastructure. The situation is worse in the digital environment. This contradicts the Constitution of South Africa, which promotes that records must be stored where transparency is promoted. Indeed, South Africa's laudable attempts to legislate and regulate digital records are not without their shortcomings. Katuu (2015) provided a summary of these efforts by stating that the NARSSA first published a set of policies and guidelines for managing digital records in 2000 and revised them in 2006. From the early 2000s, the NARSSA sought to assist public sector institutions in managing their digital records more efficiently. However, the transfer of digital records from public institutions into archival custody has not happened in any systematic manner because the national archival system has struggled to effectively manage such records and facilitate their long-term preservation (Katuu & Ngoepe 2015). Even before the emergency of cloud computing as option, the transfer of digital records from public institutions into archival custody has not happened in any systematic manner.

Research methodology

This qualitative case study utilised interviews and document analysis as data collection tools. The study was not informed by predetermined variables, but the researchers explored a phenomenon with an open mind depending on the opinions and response of participants to draw inferences and formulate a framework. The target sample of this study constituted of chief information officers (CIOs) and archive or records practitioners purposively selected from the national government departments. These officials have expertise in their respective areas of competency, for example, IT and records services within their organisations. The CIOs have capability to influence the virtual storage of the organisation's records, whilst the records practitioners are responsible for the footprints of the organisation by ensuring that records are stored and remain authentic. In the evolution of technology, records practitioners rely on CIOs to intervene when storage formats change. National government departments that have implemented some of the electronic services such as the Department of Sports, Arts and Culture, Department of Home Affairs, the Department of Science and Technology, as well as the Department of Basic Education were targeted. In this regard, 12 participants were interviewed. Furthermore, an official from the NARSSA of South Africa was also chosen as NARSSA is charged with the statutory regulatory role of records management in governmental bodies. So is the State Information Technology Agency (SITA), a public sector ICT company established in 1999 to consolidate and coordinate the state's information technology resources in order to achieve cost savings through scale, increase delivery capabilities and enhance interoperability. Interview data were augmented through document analysis of legislation and policies pertaining to data storage. The interviews for this study were arranged according to the objectives and, where necessary, follow-up questions were asked to obtain the in-depth information. As the participants were guaranteed anonymity and confidentiality, their names were coded as Participant A, B, C and so on. All the interviews were conducted in English at the participants' workplace at a date and time they determined appropriate. Only one participant declined to be recorded, but offered to speak slowly in order to give the researcher the opportunity to take notes. To provide quality to the study, questions were asked randomly depending on the responses provided by the participants. The legislation that has an impact on cloud storage was analysed to augment interview data. Data were analysed thematically and interpreted in accordance with the objectives of the study. In some instances, interview information is presented verbatim.

Ethical consideration

The study received ethical clearance from the University of South Africa's Department of Information Science Ethics Review Committee. (Reference number: 2018-DIS-0006).

Findings and discussions

This section provides an interpretation and a discussion of the findings presented in line with research objectives of this study.

Policy and legislative framework

The objective was intended to establish the policy and legislative framework used to store records in the cloud. Legislative framework plays a crucial role in the digital storage of the public sector. It ensures the protection of records from being damaged or used wrongly by unwanted sources. Digital storage must be guided by legislation and international standards of records management to ensure reliable governance. A lifecycle approach to the management of digital materials enables successful curation and long-term preservation, which should be performed within the ambit of legislation. Findings of this study revealed that the government departments do not have a specific legislation to govern cloud storage. Participant A, a CIO, indicated that his department consults various pieces of legislation with regard to cloud storage.

When asked to identify legislation that has a bearing on records storage in the cloud, participants indicated that although the *NARSSA Act* has overall bearing on record-keeping, they do not necessarily follow legislative framework but internal ICT policies. For example, Participant J explained that:

> 'Currently, we do not have a specific legislation for cloud storage, but there are various pieces of legislation that are applicable like ECT Act (it has provisions on how you manage digital records/data), the NARSA itself has some bearing on how public records must be managed. Other legislation like POPI and PAIA also make provision for management of records. Ideally, as a country we need to get to a point where we develop some legislation specifically about cloud. So you have to read the bits and pieces of legislation to make clear way on how to approach the cloud issue. If you look at SITA Act, there are mandatory services from SITA like networks. Now SITA is implementing the government cloud, which means we are now forced to use SITA cloud. Therefore, you need to read various pieces of legislation in order to come up with a business case for your environment'. (Participant J, IT Manager, 03 April 2019, Pretoria)

Other pieces of legislation identified include *ECT Act*, *Promotion of Access to Information Act* and *Protection of Personal Information Act*. Upon analysis of the legislation, the *NARSSA Act* makes only two provisions for the management of electronic records in terms of *section 13(2)(b)(ii)* and *section 13(2)(b)(iii)* that the national archivist shall determine the conditions subject to which electronic records systems shall be managed and the conditions under which records may be reproduced electronically. The first provision is about the system for the management of electronic records, whilst the second is about imaging or conversion of paper-based records into an electronic system. The Act is silent about custody entrusted to a third party such as cloud storage. An interview with a participant from the NARSSA and SITA revealed that the NARSSA has not yet issued directives to government departments with regard to cloud storage. This implies that the discretion lies with the relevant department regarding whether to entrust their records to the cloud or not. There is also no guiding document that is available for government departments in this regard. The participants agreed that the *NARSSA Act* supported digital records in conditions where the records are in devices like computers and servers that are stored securely on the government premises. Participants from IT sections indicated that the use of cloud services, such as email hosting, was taking place without the support of legislation. According to McLeod (2019), three strategies for preserving records in the cloud involve the service provider to assume preservation responsibility, building a framework for preservation and access that can be implemented through a series of interconnected but independent services and, lastly, harnessing emerging blockchain technology. However, the participants from both IT and registry sections revealed their reliance on *ARSSA Act*, which was considered outdated because it focused on microfilm, audio-visual and paper-based records that are securely locked on government premises. Kuiper et al. (2014) cautioned that storing records in such manner does not promote the rollout of e-government services, which is envisioned by the South African government.

Storage and preservation of records in the cloud

The DCC lifecycle model indicates that digital storage and preservation are necessary in the life of a record. In this objective, it was revealed that government departments store digital records on computerised devices that are safely locked on the government premises. This method of storage has contributed to the mushrooming of more than one registry in the government departments. Ngoepe and Van der Walt (2010) pointed out that decentralised registries are usually established if there would be unnecessary delays in accessing files if they were not kept near individuals working with them. However, decentralised registries can give rise to inconsistent systems and records management practices and duplication of files. In relation to this study, this type of storage isolates the citizens that stay far away from these storage premises.

The participants indicated that they prefer to store records on government premises to avoid transgression of archival legislation. However, there were those like Participant L, an IT manager, who indicated that he stores his personal records in the cloud such as Google Drive and sometimes even work-related records. However, record managers admitted to keeping records in platforms such as Dropbox, but were not aware that those were cloud storage.

Contrary to the fears of using the cloud, participants holding senior positions in IT indicated that they have email services hosted by the CSP. They have entered into service-level agreements on behalf of their departments with the CSP where they are billed for their allocated space. However, because of mistrust of privately owned cloud, the participants mentioned that they store personal information in privately owned clouds, but do not want to risk government records by storing it in privately owned clouds, for example, Dropbox. The participants listed some of the following factors that create hindrances when considering migration to the cloud adoption:

- Lack of cloud legislation
- Bankruptcy of the service provider
- Enemy of super powers
- Lack of trust in third party
- Selling of personal information
- Hindrances of cloud were on sovereignty
- Cross-border jurisdiction
- Loss of control over records

Despite the advantages from a business perspective, cloud computing also presents challenges, particularly regarding the mistrust of users to put their data on computers that they cannot control. Participant D, an IT manager, indicated that:

> 'We prefer to have control over our information to prevent fraud, misuse, etc. We also need access to the information whenever required so any interruptions or delays, e.g.: retrieval downtimes, may hamper activities. Location and access to cloud servers remain a barrier, as well as managing the destruction, retention, backup and migration processes'. (Participant D, IT manager, 14 April 2019, Pretoria)

Similarly, Obrustky (2016) pointed out that security is synonymous with cloud storage in view that records could be stolen or viewed by unauthorised people. The risk increases when customers are not in control of their records. However, Galloway (2013) suggested that following handing over of records to the cloud service provider, data transfer using encryption technology must be considered.

Participant F, an IT manager, indicated that because of a lack of cloud storage policy, records could not be entrusted to the cloud. The participants suggested that only when SITA is in charge could they move records to the cloud. This is informed by that SITA is a known agency responsible for ICT matters for the government. Currently, there is no policy or prototype guideline to advise regarding the ownership of data, security, availability of service (downtime and uptime), location of the cloud servers, backup and recovery and legal hold or e-discovery, to mention just a few issues. The concerns raised were not only limited to technology but also included organisation management, human behaviour, regulation and records management, as the participating CIO, revealed that they experienced a number of nontechnology issues with cloud computing, including a lack of control over employees' cloud computing use, a lack of internal regulations on cloud computing use, implementation difficulties, and a lack of transparency of providers' service.

Whilst security risk continues to be the paramount factor impeding cloud adoption, Participant F, an IT manager, indicated that integrity and security could be achieved by:

> '... ensuring the cloud storage complies with ISO standards. In this regard we can conduct regular compliance tests/audits to ensure there are no breaches and have a quality control process built into the workflow to authenticate records'. (Participant F, IT manager, 22 March 2019, Pretoria)

Other mitigating factors mentioned by participants include: use of strong passwords, knowing legal obligations and retaining ownership.

Framework for digital curation of records in the cloud

Based on the findings, South Africa does not have a policy or legislative framework for cloud storage. This study proposes a framework in Figure 1, which is made up of the following elements: cloud legislation and policy framework, preservation, storage and disposal. Central to this proposed framework is digital curation of records. The line outside

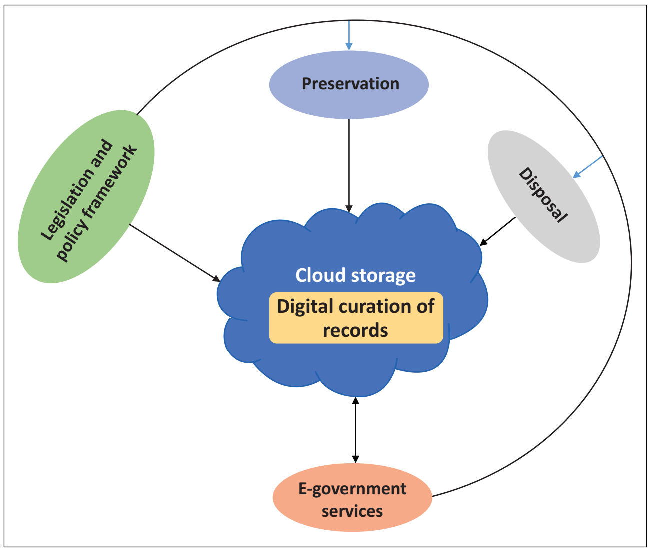

FIGURE 1: Framework for digital curation of records.

the figure shows how cloud legislation has influence over other elements and ultimately at the provision of e-government services. The arrows inside have been used to show how they relate to one another. All those coming from the legislation and policy framework indicate the influence that legislation has on each element that supports digital curation of records. The reliability of the system is dependent on the IT infrastructure, for example, LAN/WAN provided by the IT section and compliance with documents uploaded by the records management practitioners. The framework anticipates providing virtual access as digital preservation ensures that the content in digital format remains accessible over time, reliable and authentic. In the event that records are not accessible, the IT section and the records management division will work together to resolve the glitches.

Legislation and policy framework: Given the proliferation of ICT, records need to be accessed virtually by the citizens of the country in a time convenient to them. However, there is a need for cloud legislation that makes provision for cloud storage. According to Ngoepe and Saurombe (2016), legislation has a huge impact on how records are stored in any country. Franks (2013) also argued that an effective records management programme should comprise records management policy and procedures, well-trained personnel, advanced information systems and reduced risks within the records management environment. As reflected in the framework, the implementation of this legislation should be driven to all government departments, nationally and provincially by the NARSSA, which is charged to manage government records. The legislation makes provision for the migration of born digital and digitalised records to the cloud. The Act should prescribe how the current records are digitalised in preparation for migration to the cloud. Issues to be included in the legislation include but are not limited to: governance of data, compliance, especially with regard to the jurisdiction of cloud service provider, trust, architecture, access management and software isolation, incident response and availability in case a court orders a seizure of equipment (Cunningham 2015).

Cloud storage: The government has born digital and digitised records stored on computer devices that are safely locked on government premises. This storing method supports digital curation of records only in a local environment. The use of these devices limits access of the citizens to information from anywhere at any time. Obrustky (2016) pointed out that one key advantage of cloud storage is that the organisations can access information from any location, even if they do not have access to their organisation's network. Introducing cloud to the government would fulfil what Paquette et al. (2010) indicated as former president of the United States of America, Barak Obama, emphasised that cloud computing, which offers cloud storage is capable of opening up the government to its citizens. Storing records in the cloud opens the government to the citizens through e-government services. However, the government does not have a state-owned cloud storage. The current option that the government has for cloud storage is to use the CSP. However, the government's chances to control CSPs on how to use its cloud are minimal as the providers have their own rules. This creates suspicion in using the CSP when considering that the service provider could be entangled in a legal battle leading to the loss of records. The viability of the cloud has been noticed when various government departments hosted their electronic mail services with CSP in order to communicate anywhere at any time. The government, through SITA and NARSSA, should develop a state-owned cloud where all government departments can subscribe storage spaces. Stuart and Bromage (2010) pointed out that whilst the widespread usage of cloud is not common, some governments such as United Kingdom have developed a secure cloud infrastructure named G-Cloud for public sector bodies. The migration can commence with the already digitalised and born-digital records stored on computer devices.

Destruction and preservation: This stage is about disposal of records, which according to *NARSSA Act*, consists of destruction and permanent preservation of records. The current way used by the government to dispose is performed on the government premises. Stuart and Bromage (2010) opined that secure retention and disposal of records is for most organisations a legal requirement. This is necessary to demonstrate not only that those records were legally disposed but also how it was performed. In the case of disposal in the form of preservation, access is limited to those who can reach the physical archival holdings, where those records are safely locked and full access is not given to everyone. It is preferred that the digitalisation and disposal committee section guide the process. The records need to be curated digitally and accessed in a cost-effective way. Digital records of enduring value, once identified as such by NARSSA, should be transferred to the cloud created by SITA and managed by NARSSA. Such records can be made accessible to the public online. Records of ephemeral nature that are entrusted to the cloud can be destroyed once they are no longer needed by a government department.

E-government services: Records entrusted to the cloud facilitate e-government. Contribution of cloud storage to e-government services has the potential to merge distance and space, as well as reduce time, which makes the transactions of public service more effective. According to Bouaziz (2008), popular roles of e-government services allow collaboration of the government and its citizens and enable inter-agency relationship. All the records that are digitally curated can be accessed as determined by the digitalisation and disposal section. The vision of the South African government is to improve government services through government services that are protected by the law. Furthermore, there will be a huge improvement in accessing information through e-government services if this framework were to be implemented. This area depicts the public access to records or interaction between government and citizens.

Failure to address the situation will mean that records management is isolated from citizens and the world because the records are accessed manually by visiting the storage premises.

Conclusion and recommendations

This study has demonstrated the lack of infrastructure for curation of digital records, which has been equated to shortage of rain. The study argued that cloud storage offers hope to archivists to address the shortage of records storage. Cloud storage offers the accessibility of records irrespective of time and distance. The study investigated legislation and policy framework of cloud storage and digital curation of public records in the cloud. The *National Archives and Records Services Act of 1996* is the primary legislation for records management in South Africa, and it was revealed that it does not make provision for cloud storage. It is clear from the discussion that current archival legislation was created with paper records in mind, demonstrated by the rule that all records should be saved for 20 years. As technology progresses at an increasingly rapid rate, this is no longer tenable. To avoid consulting various pieces of legislation when considering cloud storage, the government, through SITA and NARSSA, should update the *NARSSA Act* to make provision for cloud storage. This is so because the study revealed that public sector officials are hesitant to migrate to the cloud for digital curation, as it is not legislated. As the South African legislative and regulatory instruments are still largely based on the principle of territoriality (Katuu & Ngoepe 2015), the concern for the participants is the loss of control over public records held by cloud providers. Indeed, whilst the cloud storage option holds many attractions, the complications that may occur as a result of the services being provided from disparate geographical locations that are subject to different legal jurisdictions may result in unexpected but significant legal consequences and need to be carefully considered in determining whether cloud computing is an appropriate option. In this digital age, organisations need awareness of cloud storage in order to create space for other activities within the organisation. Following the updating of the *NARSSA Act* to cater for cloud storage, government departments can develop policies and procedures.

Because of the lack of infrastructure for management and preservation of digital records for the purpose of increased storage and access, this study recommends that government departments should cautiously consider exploring the possibility of storing their records in a trusted digital repository cloud as an interim solution whilst observing legal obligations. As cloud storage is not very prevalent amongst government departments in South Africa, given the present challenges in managing digital records, it would be advantageous to have cloud storage tested rigorously before public entities embark on the exercise. Paper-based records can also be converted to digital objects and stored in the cloud. This will help to alleviate the problem of space and provide accurate access to records in the public sector in South Africa. It emerged from this study that in the event the government thinks of cloud storage, the services of a third-party cloud have to be purchased from the third-party provider. The records practitioners are uncomfortable with using third-party cloud because of security and legal issues. The study revealed that the government departments are confident to use the cloud storage in which the government is involved. Therefore, the government, through SITA, should consider developing a state-owned private cloud and allocate storage spaces for government departments.

Acknowledgements

The authors acknowledge the participants of this study.

Competing interests

The authors have declared that no competing interests exist.

Authors' contributions

A.S. and M.N. conceptualised the study. A.S. conducted literature review, collected data and wrote the article. M.N. supervised the study.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability statement

The data that support the findings of this study are available from the corresponding author, M.N., upon reasonable request.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Bazi, H.R., Hassanzadeh, A. & Moeini, A., 2017, 'A comprehensive framework for cloud computing migration using meta-synthesis approach', *The Journal of Systems and Software* 128, 87–105. https://doi.org/10.1016/j.jss.2017.02.049

Bhandari, A., Gupta, A. & Das, D., 2016, 'A framework for data security and storage in cloud computing', Article Read at the International Conference on Computational Techniques in Information and Communication Technology, New Delhi, 11–13th March.

Bouaziz, F., 2008, 'Public administration presence on the web: A cultural explanation', *The Electronic Journal of e-Government* 6(1), 11–22.

Carter, L. & Bélanger, F., 2005, 'The utilization of e-government services: Citizen trust, innovation and acceptance factors', *Information Systems Journal* 15(1), 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x

Cunningham, A., 2015. 'Postcustodialism', in L. Duranti & P.C. Franks (eds.), *Encyclopedia of Archival Science*, pp. 274–278, Rowman & Littlefield, London.

Cunningham, A., 2019, 'Exploring digital preservation in the cloud', in L. Duranti & C. Rogers (eds.), *Trusting records in the cloud*, pp. 179–206, Facet Publishing, London.

Duranti, L., 2005, *The long-term preservation of authentic electronic records: Findings of the inter PARES project*, Archilab, San Miniato.

Franks, P.C., 2013, *Records and information management*, Neal-Schuman, Chicago, IL.

Galloway, J.M., 2013, 'A cloud architecture for reducing costs in local parallel and distributed virtualised cloud environments', PhD thesis, University of Alabama, Alabama.

Head, B., 2013, *When rain clouds gather*, Waveland Press, Inc., Long Grove, IL.

Higgins, S., 2011, 'Digital curation: The emergence of a new discipline', *International Journal of Digital Curation* 6(2), 78–88. https://doi.org/10.2218/ijdc.v6i2.191

Katuu, S., 2015, 'Managing records in South Africa's public sector – A review of literature', *Journal of the South African Society of Archivists* 48(1), 1–13. https://doi.org/10.17234/INFUTURE.2015.16

Katuu, S. & Ngoepe, M., 2015, 'Managing digital records within South Africa's legislative and regulatory framework', in B.E. Popovsky (ed.), *Proceedings of the 3rd International Conference on Cloud Security and Management ICCSM*, pp. 59–70, Academic Conferences and Publishing International Limited, Tacoma, WA.

Kuiper, E., Van Dam, F., Reiter, A. & Janssen, M., 2014, 'Factors influencing the adoption of and business case for cloud computing in the public sector', viewed 18 December 2019, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.981.4981&rep=rep1&type=pdf

Leveille, V., 2015, 'Cloud archives', in L. Duranti & P.G. Franks (eds.), *Encyclopaedia of archival science*, pp. 136–139, Rowman & Littlefield, New York, NY.

McLeod, J., 2019, 'The cloud – Challenges and issues', in L. Duranti & C. Rogers (eds.), *Trusting records in the cloud*, pp. 13–36, Facet Publishing, London.

Neelima, M.L. & Padma, M., 2014, 'A study on cloud storage', *International Journal of Computer Science and Mobile Computing* 3(5), 966–971.

Ngoepe, M., 2012, 'Fostering a framework to embed the records management function into the auditing process in the South African public sector', PhD thesis, University of South Africa, Pretoria.

Ngoepe, M., 2017, 'Archival orthodoxy of post-custodial realities for digital records in South Africa', *Archives and Manuscripts* 45(1), 31–44. https://doi.org/10.1080/01576895.2016.1277361

Ngoepe, M. & Saurombe, A., 2016, 'Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African development community', *Archives and Manuscripts* 44(1), 24–41. https://doi.org/10.1080/01576895.2015.1136225

Ngoepe, M. & Van der Walt, T., 2010, 'A framework for a records management programme: Lessons from the Department of Cooperative Governance and Traditional Affairs in South Africa', *Mousaion* 28(2), 83–107.

Obrustky, S.T., 2016, *Cloud: Advantages, disadvantages and enterprise solutions for business*, Eastern Institute of Technology, Hawke's Bay.

Paquette, S., Jaeger, P.T. & Wilson, S.C., 2010, 'Identifying the security risks associated with governmental use of cloud computing', *Government Information Quarterly* 27(3), 245–253. https://doi.org/10.1016/j.giq.2010.01.002

Park, S.C. & Ryoo, S.Y., 2012, 'An empirical investigation of end-users switching toward computing: A two-factor theory perspective', *Computer in Human Behaviour* 29(1), 160–170. https://doi.org/10.1016/j.chb.2012.07.032

Pearce-Moses, R., 2019, 'Inter PARES trust terminology', in L. Duranti & C. Rogers (eds.), *Trusting records in the cloud*, pp. 267–286, Facet Publishing, London.

Pickover, P. & Harris, V., 2001, *Freedom of information in South Africa: A far off reality*, South African History Archive, Johannesburg, viewed 14 December 2019, from http://www.wits.ac.za/saha/publications/FOIP_1_4_PickoverHarris.pdf

Rajan, R.A.P. & Shanmugapriyaa, S., 2012, 'Evolution of cloud storage as cloud computing infrastructure service', *IOSR Journal of Computing Engineering* 1(1), 38–45. https://doi.org/10.9790/0661-0113845

Shen, Y., Yang, J. & Keskin, T., 2012, 'The evolution of IT towards cloud computing in China and US', Article Presented at International Conference on Computational Problem-Solving, Leshan, 19–21 October.

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. https://doi.org/10.1108/13590791311287337

Stuart, K. & Bromage, D., 2010, 'Current state of play: Records management and the cloud', *Records Management Journal* 20(2), 2017–2225. https://doi.org/10.1108/95656981080001364