

# **ESARBICA JOURNAL**

**JOURNAL OF THE EASTERN  
AND SOUTHERN AFRICA  
REGIONAL BRANCH OF THE  
INTERNATIONAL COUNCIL ON  
ARCHIVES**

**Volume 40**

**2021**

ISSN 2220-6442 (Print), ISSN 2220-6450 (Online)

<https://dx.doi.org/10.4314/esarjo.v40i1.1>

# CREATION AND STORAGE OF RECORDS IN THE CLOUD BY ZIMBABWE OPEN UNIVERSITY

**Godfrey Tsvuura & Kudzai D Mbawuya**  
Zimbabwe Open University, Zimbabwe  
tsvuurag@zou.ac.zw / mbawuyak@zou.ac.zw

**Patrick Ngulube**  
University of South Africa, South Africa  
ngulup@unisa.ac.za

Received: 5 November 2020

Revised: 31 March 2021

Accepted: 30 June 2021

## Abstract

This study investigated the challenges and prospects of creating and storing records in the cloud by Zimbabwe Open University in Zimbabwe. Like other universities in Zimbabwe, the university adopted Education 5.0 advocated by the government in 2019. Consequently, the university came up with innovation hubs and industrial parks that became centres for records creation. Keeping all records in the computer without appropriate backups and servers has consequences such as losing vital records. Organisations around the world use cloud computing increasingly to address records storage and disposal. Adoption of cloud computing services carries with it cost implications, and legal and ownership challenges as the virtualised environments are hosted and managed by third parties. The objective of this study was to examine the management, operational, legal and technical issues surrounding the storage of records in the cloud, and the implications for their trustworthiness and authenticity. The study adopted a qualitative research design and drew data from interviews with key participants. Qualitative data were organised into broad themes and the content reported in narrative form. The study found that Zimbabwe Open University is not using cloud computing services effectively and is in the trial phase of cloud computing. It further found that there was a lack of collaboration between the information and communication technology and the records management units as the university decided to move to the cloud on a full-scale basis. The study recommends that the university should first address the management, operational, legal and technical issues surrounding the storage of records in the cloud before implementing the complete use of the cloud. The study deepens the understanding of cloud computing in the management of records at the university, and other state universities in Zimbabwe can use this study to deal with the management of records in the cloud.

**Key words:** Cloud computing; Education 5.0; innovation hubs; industrial parks; records management; Zimbabwe Open University

## Introduction

Cloud-based records services have become an important topic in many organisations due to the benefits it can provide to businesses and their operations (Duis 2014:2). This study investigated the challenges and prospects of creating and storing records in the cloud by the Zimbabwe Open University (ZOU) in Zimbabwe. The university adopted Education 5.0 advocated by the Government of Zimbabwe in 2019 (The Doctrine, 2019). Under this drive, the university came up with innovation hubs and industrial parks that become centres for records creation. In the process, the university adopted business information systems such as the Academic Registry Information System (ARIS), Microsoft 365 and myVista to perform academic and administrative tasks (ZOU Strategic Plan 2019–2023). Cloud computing is increasingly being used by organisations around the world, and universities are no exception. The flexibility of this new technology allows the university to use cloud computing services to store records in the cloud, and then retrieve and use them at appropriate times. Adoption of cloud computing services carries with it cost implications, and legal and ownership challenges as the virtual environments are hosted and managed by third parties.

## Background and context of the study

The International Data Corporation [IDC] (2014) estimates an exponential growth of computer-related information technology (IT) infrastructure. This was a dream come true for many organisations, universities included. Today, ZOU's records are increasingly created digitally via email, spreadsheets, word-processed documents, photographs, PowerPoint presentation slides and on the website. As the university is geographically spread over all the 10 provinces and some districts in Zimbabwe, it is prudent for it to adopt cloud computing to deal with problems of infrastructure, as well as an inadequate number of lecturers. In its 2020–2023 strategic plan, the institution adopted the open and distance electronic learning (ODEL) strategy, where much of its teaching would be done through online services such as online submission of assignments, electronic marking, videoconferencing and electronic learning, among others (Zimbabwe Open University 2019). In addition, the university adopted other business information systems such as ARIS, Microsoft 365 Outlook for email and myVista for managing and storing students' records of academic work. The use of electronic services by the university is in line with the evolving use of technology in many institutions of higher learning. The myVista platform facilitates the interaction between students and lecturers; as well as access to modules; examination results; assignments and other electronic library resources. It also facilitates the interaction when lecturers upload and download assignments for electronic marking (e-marking) and provide feedback to students.

ARIS, on the other hand, facilitates the capturing of students' records upon enrolment and the automatic allocation of personal identification numbers (PIN), commonly known as student numbers. Records officers use the ARIS software when creating and managing student records and profiles. ZOU has 10 regional centres and the system allows connection between regional offices and the national centre in sharing students' information. It allows the capturing of biographical data on application forms, and students can apply by downloading the application forms from the website, complete and submit them electronically. The system is divided into regional databases that capture students' information and synchronise it to the main database at the national centre in Harare. ARIS is able to generate confirmation of registration as proof that the students are registered. The university also uses Pastel Evolution software that facilitates the payment of student fees and audit requirements. These electronic

services platforms are introduced to enable students to interact with the university without having to visit its offices physically.

All these business information systems are creating records, and such records are kept on computer servers and accessed using the internet and web browsers. While the university acknowledges the creation of records using technology, management of these records is now in cloud storage. According to Richards (2014), cloud records storage is a form of IT provision that treats computing as a set of services that can be purchased on demand through networks. McLeod and Gormly (2017) argue that organisations cannot avoid working in the cloud because records are being stored in the cloud, either by design or by default. This issue of cloud records storage becomes the most important concern for archivists and records managers. Solanki (2012) states that every new technology brings with it advantages and disadvantages, and cloud computing is no exception. Mosweu, Luthuli and Mosweu (2019:1) argue that organisations can adopt cloud-based services as they offer efficient and cost-effective services.

The challenges of cloud computing were predicted by Evans and Gustafson (1975) when they admitted that computer innovations might someday affect the way in which records and archives would be managed. Ahuja, Mani and Zambrano (2012) predict that cloud computing's popularity will be such that 80 per cent of businesses will have moved to the cloud by 2020. According to Duis (2014:6), this migration to the cloud will either involve an organisation choosing to use software as a service (SaaS); customer use of service provider applications platform as a service (PaaS); the installation of customer application on the service provider infrastructure; infrastructure as a service (IaaS) and the supply of a service provider's infrastructure to customers. Yakel (2001) examined the changing nature of records as they move to cloud-based storage services and found that as records move to the cloud-based storage services, their nature changes. Scholars such as Ngoepe and Saurombe (2016), Katuu and Ngoepe (2015a), Katuu (2015a), Duranti (2013b), Miller (2011), Alfresco (2011) and Spring (2011) embrace that records professionals must be diligent to ensure that their agencies adopt appropriate records management policies and procedures when cloud computing services are contracted in order to satisfy record-keeping requirements. There are specific issues that records professionals need to address when confronted with cloud computing, such as jurisdiction, control, custody and trust (Duranti 2013a:51). Of the challenges facing the management of digital records, particularly in the cloud environment, the legal and regulatory framework has been given the least attention, particularly by records professionals (Katu 2015b:296). Cloud computing, therefore, challenges the fundamental tenets held by records professionals on custody, ownership, authenticity, context and preservation (Duranti 2013a:47). The International Standards Organisation (ISO 15489-1) (2016) provides a framework for any organisation to adopt and use to manage its records. Cox (2001) points out that the role of records management in all organisations is ensuring accountability and providing evidence of transactions and decisions. The concern for records professionals is the loss of legislative and regulatory control over records held by cloud providers (Katu & Ngoepe 2015b). The uptake of cloud computing is one of the key components of the information and communication technology (ICT) strategy across many organisations (NSW Government Cloud Policy 2015). This means that even when records are kept in the cloud, they still support the evidential aspects of good governance in organisations.

## Cloud-based services for records management in ZOU

Cunningham and Wilkins (2009), James (2010) and Ferguson-Boucher (2011) note increased interest in the cloud-based records services in the records profession. Cloud-based services are the services that are provided to users through the internet by service providers (Kale & Mente 2017:140). Cloud-based records services include online storage, backup solutions and document collaboration services. The service of cloud computing is internet based whereby resources such as software and information are provided to computers and other devices on demand (NSW Government Cloud Policy 2015). They are designed to provide easy and scalable access to web-based applications, resources and other services that protect the records from abuse.

Mosweu et al. (2019) hold that cloud-based records management enables convenient, on-demand network access to a shared pool of configured computing resources. The cloud itself is a virtualisation of resources such as networks, servers, applications, data storage and other services. Universities and other organisations throughout the world are moving to cloud-based records management to cut costs, eradicate redundancies and pool resources. However, when choosing to use cloud-based services, every organisation has to weigh it up against the risks associated with the privacy and security of its records. Stuart and Bromage (2010) argue that records managers need to be aware of many factors that could affect control of their records negatively. These factors include the likelihood that their records might be stored in unknown locations; the potential problems that might occur when applying retention and disposal schedules to the cloud-based records; the possibility of not being able to export data stored in the cloud; and the potential privacy and security risks that could result from using cloud-based records management (Duis 2014:6).

### Benefits of cloud records storage services

Organisations started to use the cloud-based services increasingly to offer efficient and cost-effective technology solutions (Duis 2014:6). The flexibility of the new technologies allows organisations to use cloud-based applications provided by service providers through various networks. According to Kale and Mente (2017), cloud computing is becoming an adoptable concept for the educational area, with dynamic scalability and usage of virtualised resources as a service through the internet. Benerjee (2009) holds that cloud computing provides storage facilities through the network, and data are stored in local storage of service providers who provide online storage space. Kale and Mente (2017) also mention that cloud computing is a type of outsourcing of computer programmes and networks, using the 'cloud', which means that people do not have to worry about things like storage media and power; they can simply access the end results. In fact, when people talk of cloud computing, they are talking about the internet and networks that are able to store records that can be accessed at any time via web-connected devices. Creeger (2009) notes that most organisations found shifting to 'the cloud' to be both cost-effective and operationally straightforward. Kale and Mente (2017) state that cloud computing enables users to manage, share and access data through the internet. Scholars such as McAfee (2009) argue that the movement to the cloud is inexorable. Carr (2008) compares this to the shifting from steam power to electrical power during the late nineteenth and early twentieth centuries.

In the United States of America, *InformationWeek* (2009) reports that the Obama administration made cyber infrastructure, in general, and cloud computing, in particular, key

priorities for the federal sector. Lewin (2009) states that the federal government adopted the 'cloud computing initiative', outlining both the rationale for the initiative and some key components, such as its major characteristics, its delivery methods and its deployment models. On the subject of records and archives management, the National Archives and Records Administration (NARA) (2011) suggests that agencies should be aware of the potentially adverse effects of cloud computing on records management work. Cloud computing sometimes seems straightforward from the point of view of IT costs and service provision, but its benefits for records management are murkier (Richards 2014). McLeod (2003) holds that in addition to providing evidence and ensuring its accountability, an organisation has the responsibility to manage its records so that it can support the continuing conduct of its business and remain compliant with its regulatory requirements.

In cloud computing, all users of the institution are connected to the cloud and individual login or ID is provided to all users for their respective tasks. Lecturers can upload assignments, tutorial letters, video lectures, coursework marks and other learning materials, and the students can access all the data and information provided through the internet using laptops, desktops and other electronic devices such as smartphones anywhere and at any time. Kale and Mente (2017) state that through cloud computing it becomes possible for lecturers to analyse students' records, as these will be kept directly on the internet by all university users. They added that cloud computing provides the following benefits:

- **Personalised learning:** Using cloud computing enables students to access and share a wide array of resources, access data anywhere and at any time, and enrol in online classes and participate in group work activities.
- **Cost-effectiveness:** There is no need to buy hardware and software as cloud computing provides a virtual environment at a lower cost.
- **Service availability:** Users can access stored data on the cloud at anytime and anywhere, independent of any location.
- **Low maintenance:** Virtual infrastructure reduces maintenance costs nearly to the negligible.
- **Storage capacity:** It stores far more data for any cloud user than any other storage device.
- **Security:** The cloud system provides confidentiality, data integrity and privacy, so only an authorised user can access stored data.
- **Performance:** Cloud computing enables the cloud user to customise the system configuration by sharing infrastructure, so it increases the speed and performance of the system.
- **User-friendly and Go Green:** The cloud service facility is very easy to use, and it surely reduces the carbon footprint.

Richards (2014) states that individuals and businesses can use as much of the service as they need without having to make large infrastructure investments, which may become idle when computing needs are less than maximum capacity. One of the benefits of cloud computing, as Creeger (2009) states, is economic sustainability because it allows organisations to make use of large amounts of computing power without much investment in IT. This allows computing infrastructure, hardware and software to be treated as largely modular services that can be scaled up and down easily and with minimal ongoing interaction and negotiation with the computing resource provider (Richards 2014). It also allows organisations to minimise the number of IT professionals necessary to meet the IT needs of the organisation (Richards 2014:14).

## Statement of the problem

ZOU is in the trial phase of moving its records to the cloud storage services. However, there are some hurdles that need to be overcome first before the benefits of cloud records storage services can be enjoyed. Mosweu et al. (2019:1) outline that issues related to records storage, jurisdiction, privacy, security and digital divide are a challenges that need to be surmounted to benefit fully from cloud-based records management services. Duranti and Rogers (2012:529) argue that a move to the cloud could mean a loss of control where interruptions in the service may make records inaccessible, and there may be a lack of clarity about where the records are stored. Despite the challenges mentioned, ZOU is moving towards cloud-based records services as it adopts the ODeI mode of learning. It is against this background that the study sought to highlight some important issues that need to be addressed first before the institution can enjoy the benefits of cloud-based records services.

## Purpose and objective of the study

The main purpose of this study was to investigate the challenges and prospects of creating and storing records in the cloud by ZOU in Zimbabwe. Specifically, this study intended to answer the following questions:

1. Is ZOU transitioning to cloud records storage?
2. How can a service provider be trusted as a neutral third-party record-keeper?
3. How does ZOU establish the authenticity, continuing identity and integrity of the records and archives stored on the cloud?
4. How is authenticity and trustworthiness guaranteed when storing records in the cloud?

## The conceptual framework of the study

A conceptual framework may be based on the concepts in the extant literature; personal experiences of the researcher; knowledge about the context of the phenomenon and aspects of existing theories (Ngulube 2020a). The study uses digital diplomacies as its conceptual framework. This is mainly because in cloud-based services, records are being contracted to the third-party service providers who will keep such records on behalf of the organisation or outside the parameters of its control. Duranti (2009:41) describes a trusted custodian as a neutral third party who must demonstrate that it has no reason to alter or to allow others to alter the records in its care, and that it has the knowledge required for attesting to and ensuring the continuing authenticity of the records. Ensuring authenticity is key to the identity of the trusted record-keeper or custodian or, more generally, of the records professionals responsible for assessing and guaranteeing the trustworthiness of the documentary heritage over time (Duranti 2009:41). Mosweu et al. (2019) argue that cloud-based records services enable convenient, on-demand network access to a shared pool of configurable computing resources. These resources include networks, servers, storage, applications and services that can be provided and released rapidly with minimal management effort or cloud provider interaction. Cloud computing technology ensures that data, records and information are always available as they are backed up on a number of computers, which diminishes the possibility of data and application loss (Mosweu et al. 2019:3).

On the one hand, the concept of digital diplomacies defines a digital record as a digital component or group of digital components that are treated and managed as a record, or, more

specifically, a record of which the content and form are encoded using discrete numeric values or binary values of 0 and 1 (Duranti 2009:44). MacNeil (2000:52) argues that a digital record must have an identifiable context, an originator, an author, a writer, an addressee and a creator. In addition, the concept of a trusted third-party record-keeper was developed in the context of digital records storage contracting. This refers to a physical or juridical person who is trusted with the maintenance of digital records (Duranti 2009:40). To qualify as a trusted record-keeper it must demonstrate that it has no reason to alter the records and no interest in allowing others to do so, and must have the knowledge necessary to implement procedures that would ensure the integrity and accuracy of the records (Reams, Kuttan & Strehler 1997:37).

On the other hand, the theory of digital diplomatics emphasises the importance of identifying evidence (Smit, Glaudemans & Jonker 2017). All activities that records participate in are linked to each other and any omission diminishes the ability of the chain to preserve the authenticity of the records (Jansen 2015:47). In order to enable records professionals to understand digital records and be responsible for their trustworthiness over time, the InterPARES Project took traditional diplomatics and archives knowledge and applied it to all types of entities existing in a variety of digital environments, in the process, developing a new body of knowledge aimed at serving current and future needs (Duranti 2009). This new knowledge, according to Duranti (2009), was named ‘diplomatics of digital records’ and was considered to be a product of special discourses and diplomatics in the field of records and archives management. Jansen (2015) argues that within the InterPARES Projects, theory and methods are developed to be capable of ensuring the reliability, accuracy and authenticity of electronic records created in dynamic, experimental and interactive systems. Duranti (2009) effectively attempted to broaden the types of records to which diplomatics could be applied. In the InterPARES Projects (1998–2018), Duranti applied diplomatic mechanisms to investigate the veracity of records in new computerised environments (Ross 2000). Authors such as Mosweu (2020), Aslan and Goksu (2016), Ross (2000) and Smit et al. (2017) applied the digital diplomacy as a conceptual framework for their studies. Diplomats theory in this context is concerned with the issues of trust in records maintained and used in online environments. For records to be used as evidence, they need to be authentic (Duranti & Jansen 2016). To prove authenticity, the continuing identity and integrity of the records and archives must be established. Records and archives have a stable content and a fixed form, and, together with the metadata the layers of organisational archive they belong to, they reveal the legal, administrative, provenance, procedural, technological and documentary contexts belonging to identifiable organisations, persons or groups, and are linked to related records (Duranti 2009:40).

## **Literature review**

The use of cloud-based records services has many potential implications that records professionals need to be aware of when considering moving to the cloud (Duis 2014:10). Many areas of concern for records professionals that reoccur relate to the security, location, portability and retention of the records (Blair 2010; Stuart & Bromage 2010; Duis 2014). Duis (2014) argues that these concerns have similarities that they all present potential control issues for records professionals. It is important for records professionals to consider these implications because their duty is to ensure that records remain reliable, accessible, authentic and accurate (Stuart & Bromage 2010:220). The security of records is a major concern for records professionals, as any loss of control over them through unauthorised access breaches the privacy and confidentiality requirements for records (Ferguson-Boucher 2011:65). It is



always advised that records should be stored in cloud environments that provide adequate protection and that consideration should be given to whether sensitive records are to be stored in the cloud (Cunningham & Wilkins, 2009; Blair 2010; Coutinho 2012). The Ponemon Institute (2011) argues that organisations should define what constitutes sensitive records and have to be proactive in determining what records would be too sensitive to store in the cloud. If these records are not excluded from the cloud entirely, it is likely that appropriate levels of security need to be applied specifically (Barnes 2010:28).

Duis (2014) advises records professionals that the use of cloud computing impedes their knowledge of the location of the records. It is very likely that the physical location of the cloud could be in another jurisdiction (Barnes 2010:27). Accordingly, Reed (2009) and Stuart and Bromage (2010) argue that records stored in the cloud are also located on different servers leased to the service providers and it is not always possible to know the exact location of the server on which the records reside. According to Inland Revenue (2013), this creates a potential issue for records managers, since it is possible that cloud-based records might be subject to the laws of another jurisdiction. Stuart and Bromage (2010:217) argue that the incorporation of the cloud into the way organisations conduct business should not be based on a technological decision, but on a decision of examining risks to organisational records.

As ZOU is changing the way it conducts business by adopting business information systems and moving to the cloud, records personnel need to be aware of the risks associated with managing records in the cloud. As it generates more data and records, there must be confidence that they are stored in a safe cloud. McLeod and Gormly (2017) hold that the issue of using cloud service providers to store records and archives collections is particularly important for archivists and records managers. In this regard, archivists and records managers need to be confident and trust that cloud service providers are able to store their organisational records. Accordingly, McLeod and Gormly (2017) illustrate that if the cloud-based records service providers are to be used, their viability, sustainability and trustworthiness are paramount. However, it is clear that cloud computing offers good tools for organisations to conduct businesses efficiently and improve records management (Mosweu et al. 2019:1).

Blair (2010) and Sahandi, Alkhalil and Opara-Martins (2013) hold that another potential issue of control that records professionals might face is that of portability of data. Various cloud architectures lack formal technical standards governing how data are stored and manipulated in the cloud environments and this could have implications for the preservation of metadata and the possibility of being able to export data from the cloud (Duis 2014:11).

NARA (2011) notes that some cloud architectures lack formal technical standards governing how data are stored and manipulated in cloud environments, thereby threatening the long-term trustworthiness and sustainability of the data. In addition, Richards (2014) poses that a lack of portability standards might make it difficult to dispose of or transfer records in accordance with recordkeeping requirements. One risk associated with cloud computing is that organisations remain responsible for any records stored by a cloud provider (Queensland Government 2014). In their study, Sahandi et al. (2013) reveal that portability issues were common for businesses. Records managers have to be aware that there could be potential incompatibilities between applications, and plan for this accordingly (Cunningham & Wilkins 2009:30).

Duis (2014) further articulates that there are other concerns specific to records management that have potential issues, for example, applying retention and disposal requirements to records in the cloud. Blair (2010) highlights that records managers must ensure that retention requirements of records stored in the cloud can be met. If records managers are not aware of these requirements, they will not be able to dispose of such records adequately (Stuart & Bromage 2010:222). Barnes (2010) believes that cost, security, performance, availability, business viability and legal compliance must be considered before moving to the cloud. Gatewood (2009) suggests that records managers, information technologists and legal staff should work together to minimise the risks of cloud-based records services. Blair (2010) places the records and archives professionals as among the key figures in determining whether to move to the cloud, in conjunction with information technologists and other key decision-makers. This collaboration between departments must be done early so that the implications are ascertained and all involved understand what is being planned (Blair 2010:3).

The Archives and Records Management Administration (ARMA) (2010) points out that a wide range of potential records management risks are associated with cloud computing, such as potential failure to meet recordkeeping regulatory requirements; jurisdictional issues regarding data storage; vendor continuity concerns; a lack of clarity surrounding data ownership and interoperability challenges. The Kentucky State Government (2012) outlines that cloud computing has a potential impact on records and archives management. Cloud computing is a means to achieve outsourcing of records storage and presents a number of opportunities for records and information management (Queensland Government 2014). Kale and Mente (2017) state that most academic institutions have become highly dependent on IT to service their requirements. According to the Kentucky State Government (2012), cloud computing services often provide common business applications that are accessible online through web browsers, while the software and data are stored on the service provider's servers.

## **Research methodology**

The researchers adopted a qualitative research approach. Qualitative research is a form of social action that stresses the way people interpret and make sense of their experiences to understand the social reality of individuals (Haradhan 2018:2). This methodology was used to discuss qualitative aspects of the study in detail. The goal of this approach was to have a deep understanding of the issues surrounding cloud records storage. Purposive sampling was used to select subjects for data gathering. It was important that the researchers use this sampling method to select the right subjects to obtain data from. Ngulube (2020b) argues that non-probability (non-random or purposeful) sampling mostly relates to qualitative studies, and the size of typical samples in qualitative research methods is between three and 60. This study used three informants as a sample. Interviews were held with the participants and the researchers paid attention to the voice of each participant. This involved asking them questions and recording their answers. The researchers then coded the data as a first step in the analysis. Coding and categorising data helped researchers to create inventories of data and acquire deep, comprehensive and thorough insights into the data (Miles, Huberman & Saldana 2013; Saldana & Omasta 2018). The researchers used an emergent framework to code and categorise the data, and grouped them into themes. They identified segments of meanings from the data provided and labelled them as interview#1, interview#2 and interview#3. The researchers preferred to use the emergent code to make sure all data were considered for reporting.

## Findings and discussions

The findings of the study are presented and discussed in line with the research questions that guided the study.

### The use of the cloud for records storage by ZOU

The first question intended to understand the use of the cloud for records storage by ZOU. The participants were asked where ZOU keeps its records that were generated through the business information systems. The interviews with the participants indicated that not all university records were in the cloud. The participants were asked where ZOU keeps its records that were generated through the business information systems. They said that records such as students' admissions, registration and other academic records reside on the local server of the university. When asked whether ZOU was considering moving to the cloud records storage facility, interview#1 said that they were in the trial phase of moving to the cloud using internal systems, but was quick to point out that: "...there are costs, security and skills factors that need to be considered first and foremost." Interview#1 was further asked about the involvement of records personnel in the trial phase and management of the records in the local servers and said "... currently, it is the ICT manager who is responsible for the management of all information in the local servers, and the records management unit is not involved in the management of such records". Interview#1 was further asked to elaborate on the types of records that were kept on the ICT internal servers and had this to say "... records of students, their programmes, regulations, courses on offer, assignments and modules that are uploaded on myVista platform".

However, in the quest to increase efficiency in business processes, Mulauzi and Wamundila (2012) opine that records management personnel are critical in the design of appropriate recordkeeping systems and should manage records through their life cycle. The study established that the business information systems platforms such as ARIS, Microsoft 365 and myVista were housed in the ICT department, and the records management unit had little influence on the management of records generated by these information systems.

Interview#2 was asked to give more insight into the records management function in view of cloud records storage and said that "the records management unit needs the following: three-in-one photocopying; printing and scanning machine; an electronic database for all the digitised record, and a stand-alone server for the storage of all digitised records. The respondent further said that before talking of storing records in the cloud, there was a need for a database system that specialised in paper capture and document management; that enabled electronic filing and uploading of digitised records; that guaranteed data privacy/data protection, that had auditing functionalities; that does not violate the context, structure and content of the created and preserved records; that maintains the authenticity, reliability and trustworthiness of the digitised records; that mimics the physical ZOU personnel files, including those of students; that provides access, reading and retrieval of records over time, given the rapid changes in technology; that does not render the digitised records obsolete and unreadable; and that stores huge amounts of records with expandable fields and is suitable for archiving. However, ZOU is lacking behind in terms of ICT systems and as such cloud computing or keeping records in the cloud requires infrastructure and skilled personnel. The researcher was actually surprised that ICT department is in a trial phase of going to the cloud

before addressing the critical issues they are supposed to provide as outlined in section 20 of the ZOU Act.”

The participant (interview#2) was further asked to elaborate on the roles of the records management unit in view of the fact that it was not involved in the trials for moving to the cloud storage. According to the participant, “... the unit was established in 2013 as the custodian of all university records, whether paper or electronic. It has since scanned some administrative records that are kept on compact discs (CDs). What the researcher mentioned at the beginning of the interview was that the resources were needed before the university could consider moving to the cloud. Fundamental issues need to be addressed first, because moving to cloud records storage has some negative implications for the university records in terms of the legal, legislative, integrity, authenticity and access control of the records. Who will be the service provider? At what costs? And what form of a contract will there be in terms of access and control of the records?”

Interview#2 was further asked how they were managing records on CDs. The participant was quick to point out that technology is advancing and could render these CDs unreadable in the future. Interview#2 further pointed out examples of some vital records that need appropriate attention in the technological environment, such as staff files and students’ records. Rhetorically, interview#2 asked “... are students able to come back 20 years from now and get their results? These are some of the fundamental issues we need to address first and foremost, and can only be addressed when there are clear guidelines on who actually manages students’ records. Is it the ICT or the records professionals?”

Interview#3 was asked to give insights into their department in view of cloud records storage, and had this to say, “...we are the users of the business information systems. We access the records from our local computers, but the servers reside with the ICT department. The section is able to download data from, for example, the ARIS for operational activities as we admit and register students, and make reports that are required even at the ministry level. All record-keeping activities and keeping of records in the cloud are invested with the ICT department and the records management unit”.

### **How can a service provider be trusted as a neutral third party record-keeper?**

The second question was to understand the trust given to the service provider as a neutral third-party record-keeper. The participants were asked to elaborate on the use of service providers as third-party record-keepers. They said that, at that stage, the university intended to use ZOU servers or localised servers that are set in the premises.. The participants considered issues of costs and security of records given to third-party service providers. Interview#1 said, “... the current platforms such as myVista, Office 365 and ARIS are all premised within the university and no third-party service provider is involved”. However, the participant could not rule out the use of third-party service providers if the university chooses to store all university records in the cloud.

### **Establishing authenticity and trustworthiness of records in the cloud**

The third question intended to establish authenticity and trustworthiness of records in the cloud. The participants were asked how the university would establish the authenticity of the records storage in the cloud. Mosweu (2020:68) holds that authenticity of records can be maintained through the use of usernames and passwords, audit trails, built-in computer

security mechanisms, segregation of duties, and systems that do not allow records to be deleted. This is also in view of Duranti (2013b:3), outlining that, traditionally, trust in records was based on trust in those who hold them in custody. Interview#1 said it was necessary to put the policies in place and train staff before moving the records to the cloud. Interview#2 said, “there was need to put in place policies and regulations that detail the roles and responsibilities of each unit in the creation, management and preservation of the records in the cloud. Authenticity and trustworthiness of the records in the cloud need to be established first, starting with personnel managing the records, how they are preserving the records and whether the cloud service provider is a trusted and neutral somebody who will not affect the records in any way. As it stands right now, it appears there is a conflict of interest on who has official record-keeping roles and responsibilities within the university. It is a standard in records management that every employee who handles university records is responsible for following the appraisal and retention rules associated the records.”

### **Guaranteeing authenticity and trustworthiness when storing records in the cloud**

The fourth question intended to understand how authenticity and trustworthiness are guaranteed when storing records in the cloud. Mosweu (2020:64) holds that records generated by digital systems should be authentic and that such authenticity should be maintained as long as the records are used in business processes on which to base decisions. The participants highlighted a number of ways to authenticate records; for instance, the use of policies. The findings are in line with Stuart and Bromage (2010:223) who argue that organisations should introduce policies and codes of best practice in the use of cloud storage and engage trusted service providers. Policies should focus on user behaviour and address issues such as information confidentiality, integrity and access to information (Federal Departments and Agencies 2009). These policies should be formulated through open dialogue between records management and ICT units (Stuart & Bromage 2010:223). Accordingly, from the interviews conducted, the study established that the records management unit must share knowledge on recordkeeping with other stakeholders. As such, Stuart and Bromage (2010:224) outline some simple ways organisations can use to maximise their security and the management of their records in the cloud as asking where the records will be stored and processed, and trying to find jurisdictions that are complementary to their own; seeking contractual agreement to obey privacy requirements; seeking assurance that in the event of the termination of the contract, no trace of the records would be retained by the provider; and understanding how their provider backs up stored information and can restore records in case of emergency.

Kable (2010) has the view that with further standardisation of the cloud environment, including input from the records management and legal experts, good policy and possible change to legislation would be needed to address the opportunities and threats of the cloud storage. Records managers need to be involved in the decision and share knowledge on the risks and benefits of the cloud storage. According to Stuart and Bromage (2010:224), such decision should be risk based and approached with all the due diligence of any other form of distributed storage contract. The issues discussed help to authenticate records in digital environment.

### **Discussion**

The study established that ZOU had not yet used the cloud records storage facility, although one participant said they were in the trial phase. The findings of this study indicated a lack of

collaboration and coordination between the ICT and records management units. This was in view of the study revealing that, in 2016, the records management unit compiled a records digitisation policy, but is not involved in the management of all the digitised records of the university. Duis (2014:35) highlights that records managers must be closely involved in decisions relating to cloud records storage initiatives. However, this collaboration and involvement were not reflected in the data collected from the participants. According to Blair (2010), the records managers need to be involved early whenever an organisation is considering cloud records storage. A study by Kalusopa (2016:102) revealed that the depth of managing electronic records in terms of existing office systems, email management, integration of records management and ICT systems remains low. Several scholars ascribe this lack of collaboration between records management and ICT departments to the absence of organisational plans for managing digitised records, low awareness of the role of records management in supporting organisational efficiency and accountability, absence of dedicated budget for records management, absence of migration strategies and vital records, and disaster preparedness and recovery plans (Katu 2016; IRMT 2004; Brown, Katu, Sebina & Seles 2009; Goh, Katu, Miller, Nordland & Sebina 2009). Kalusopa (2016:110) also agrees that the integration or collaboration of ICT and records management is most feasible when an organisation is deciding to move to cloud records storage. McKemmish (1997) argues that this collaboration must be done, especially in cases where continuum-based thinking and practice are concerned.

The study established that digitised records in business information systems are kept on local servers of the university; hence, the security of these records is the responsibility of ICT personnel and not records managers. The study revealed that costs, security and skilled personnel, which are critical when an organisation is deciding whether to store its records in the cloud, are the major challenges faced by the university. Security of records is highlighted as a major concern for records managers, as any loss of control over records through unauthorised access, “hacking, interception and user misuse” is likely to breach the privacy or confidentiality requirements of records (Ferguson-Boucher 2011:65). On keeping records in local servers, Duis (2014), Coutinho (2012), Blair (2010) and Cunningham and Wilkins (2009) advise that records should be stored in cloud environments that provide adequate protection. There are threats associated with keeping records on local servers, such as viruses, cyber-crimes and disasters. However, this finding is in line with the views of Wang, Rashid and Chuang (2011:239) who argue that due to scepticism in data security of a cloud in the public, many organisations are implementing private clouds at their own premises. This could allow the university to design, develop and implement a customised cloud service and have full control over the records and other security concerns.

The findings imply that cloud records storage has implications for the management of records in the university. A study by Mugenyi (2018) established that in Uganda, banks adopted cloud computing technology and managed to increase their capacity to store records virtually. Cloud computing technology ensures that data, records and information are always available, as they are backed up on a number of computers, which diminishes the possibility of data and application loss (Mosweu et al. 2019:2). Even though it is clear that cloud computing offers good tools for organisations to conduct their businesses efficiently and improve records management, Mosweu et al. (2019:1) argue that African countries still experience hiccups that prevented them from fully reaping the rewards brought by cloud computing services. Nwabuonu and Nwachukwu (2014) imply that costs of ICT infrastructure, such as computers, software installation and maintenance, and cyber threats that can be experienced in keeping

records in the cloud can have negative implications for the records. Matters relating to trust in records maintained and used in online environments are also of concern.

### **Implications of cloud computing for records management in state universities in Zimbabwe**

There are a series of implications and breaches of security when storing records in the cloud. The implications include training of records personnel, cloud computing policies, appropriate coordination between ICT and records management departments, trust among all players involved in the process of cloud computing, as well as security and privacy of the records in the cloud.

This study has implications for both the case study and universities in Zimbabwe. This study underscored the need for the state universities in Zimbabwe to prepare for and be aware of the challenges experienced when using cloud computing services to store records. Mosweu et al. (2019:8) note several factors that need to be addressed before using cloud computing services, which include issues such as bandwidth, licensing, power supply, digital divide, capacity building, quality of services, ICT infrastructure needs, security and privacy concerns. The future of cloud computing remains to be seen with current issues arising in terms of the security of data; therefore, state universities need to create policies that provide security to data stored in cloud computing. Gholami (2016:iii) outlines some mechanisms and techniques that can enhance the security and privacy of data and make the cloud platforms more secure. These mechanisms and techniques include encryption, trusted platform module, secure multi-party computing, homomorphic encryption, anonymisation, container and sandboxing technologies. The issue of data ownership is a critical matter that state universities need to take into account and ensure that cloud-based solutions are in place to protect data privacy in an appropriate manner.

There are also some breaches of security that state universities need to be safeguarded against when storing records in the cloud. If there are no appropriate policies and contractual agreements between service providers and state universities, it would lead to a loss of control of the records, as cloud providers may perform data mining using clients' records, thereby compromising security in the cloud. Trust agreements must be signed between service providers and users to safeguard the records stored on the cloud. In this regard, Mosweu et al. (2019:1) state that all issues related to records storage, jurisdiction, privacy, security and the digital divide need to be overcome to benefit fully from cloud-based records management services.

### **Conclusion**

This study established that ZOU was in the trial phase of moving to a cloud records storage facility. Costs, security and skilled personnel, which are critical to the smooth movement to the cloud records storage, need attention. The study concluded that there was a lack of collaboration between the ICT and records management units as the university is deciding to move to the cloud. This is with a view to the fact that such records should be managed under the tutelage of skilled records managers to uphold the cultural (or historical) value of these records, as envisaged in the records continuum theory, and to maintain the evidential value over time. In view of the findings, this study recommends that the following:

1. ZOU should ensure the interoperability of ICT and records managers in making decisions on the use of the cloud records storage. This should be done in an early stage of the planning phase. Records are central to the administration of the university's activities as they provide evidence and allow proper monitoring of work. Therefore, coordination of ICT and records management activities within the university is an important aspect of appropriate digital recordkeeping decisions.
2. The university should raise awareness of the role of records management in supporting organisational efficiency and accountability. Therefore, such records must be in the custody of records personnel who have skills in the creation, management and disposal of obsolete records. The university should invest in the training of records and archives personnel, so that they have appropriate skills and knowledge to create and manage digitised records and archives in the cloud if the organisation decides to move to the cloud. Records personnel should know what to keep and what to discard through a records appraisal process. This process would help to discard unwanted records and only keep those that provide required evidence. This would help to reduce the costs of keeping records in the cloud.
3. The decision on whether to move to the cloud or not should involve all stakeholders and not be left to one department such as ICT. The ICT department should be a facilitator or enabler of appropriate digital recordkeeping and should not be the keepers of the records, as the records need to be appraised by the records managers.
4. The university should know or be sensitised to make sure they understand the benefits and paradox of cloud computing.
5. The university should first address the management, operational, legal and technical issues surrounding storing records in the cloud.

The recommendations made by this study have value for other higher education state institutions in Zimbabwe. They may use some of the recommendations, with adjustments, to ensure that their records remain trustworthy and authentic. This research is a case study, which implies that its findings cannot be generalised to all public universities in Zimbabwe. However, if more case studies are conducted on the subject, it would be possible to understand the creation and storage of records in a cloud more deeply and to build theory on the management of records in a cloud. The study also has implications for curriculum development. Skills for managing records in a cloud may need to be addressed.

## References

- Ahuja, S.P., Mani, S. & Zambrano, J. 2012. A survey of the state of cloud computing in healthcare. *Network and Communication Technologies* 1(2): 12-19.  
doi:10.5539/nct.v1n2p12
- Alfresco. 2011. Alfresco for cloud document management. [Online]. Available WWW: [http://www.alfresco.com/products/cloud?ct\\_id=533a2273](http://www.alfresco.com/products/cloud?ct_id=533a2273) (Accessed 12 June 2020).
- Archives and Records Management Administration (ARMA). 2010. *Guidelines for outsourcing records storage to the cloud*. Overland Park, KS: ARMA International.
- Aslan, P. & Goksu, O. 2016. Digital diplomacy, global perception and Turkey. Paper presented at 14<sup>th</sup> International Symposium Communication in the Millennium at 5–7 May 2016, in Istanbul – Turkey. [Online]. Available WWW: [https://www.researchgate.net/publication/304622106\\_Digital\\_Diplomacy\\_Global\\_Perception\\_and\\_Turkey](https://www.researchgate.net/publication/304622106_Digital_Diplomacy_Global_Perception_and_Turkey) (Accessed 14 September 2020).
- Barnes, F.R. 2010. Putting a lock on cloud-based information. *Information Management Journal* 44(4): 26-30.



- Benerjee, P. 2009. An intelligent IT infrastructure for the future. *15<sup>th</sup> International Symposium on High-Performance Computer Architecture* 14-18 February, 3.
- Blair, B.T. 2010. Governance for protecting information in the cloud. *Information Management Journal* 44(5): HT1-HT4.
- Brown, A., Katuu, S., Sebina, P. & Seles, A. 2009. *Module 4: preserving electronic records*. London: IRMT.
- Carr, N. 2008. *The big switch. Rewiring the world, from Edison to Google*. New York: Norton and Company.
- Coutinho, R. 2012. Cloud computing or cloudy computing: Are the cost savings worth it? [Online]. Available WWW: <https://www.clerkbase.com/newsletter/CloudComputing.pdf> (Accessed 25 July 2020).
- Cox, R. 2001. *Managing records as evidence and information*. Westport, CT: Quorum Books.
- Creeger, M. 2009. Cloud computing: an overview. *Acmqueue* 7(5): 1-15. [Online]. Available WWW: <http://queue.acm.org/detail.cfm?id=1554608> (Accessed 5 June 2020).
- Cunningham, P. & Wilkins, J. 2009. A walk in the cloud. *Information Management Journal* 43(1): 22-30.
- Duis, E. 2014. The involvement of records managers in cloud computing decisions: a cross-sectional study of New Zealand records managers. Unpublished MIS thesis. Victoria University of Wellington. [Online]. Available WWW: <https://researcharchive.vuw.ac.nz/xmlui/handle/10063/3398> (Accessed 5 June 2020).
- Duranti, L. 2009. From digital diplomatics to digital records forensics. *Archivaria* 68: 36-66.
- Duranti, L. 2013a. Archival science in the cloud environment: continuity or transformation? *Atlanti* 23: 45-52.
- Duranti, L. 2013b. Trust and conflicting rights in the digital environment. [Online]. Available WWW: [http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/VC\\_Duranti\\_26\\_plenary1.pdf](http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/VC_Duranti_26_plenary1.pdf) (Accessed 3 July 2020).
- Duranti, L. & Jansen, A. 2016. Authenticity of digital records: an archival diplomatics framework for digital forensics. [Online]. Available WWW: [http://www.researchgate.net/publication/290042000\\_Authenticity\\_of\\_digital\\_records\\_An\\_archival\\_diplomatics\\_framework\\_for\\_digital\\_forensics](http://www.researchgate.net/publication/290042000_Authenticity_of_digital_records_An_archival_diplomatics_framework_for_digital_forensics) (Accessed 21 June 2020).
- Duranti, L. & Rogers, C. 2012. Trust in digital records: an increasingly cloudy legal area. *Computer Law and Security Review* 28: 522-531.
- Evans, F.B. & Gustafson, M.O. 1975. The international scene: news and abstracts. *American Archivist* 38(2): 223-240.
- Federal Departments and Agencies. 2009. *Federal chief information officers. Council guidelines for the secure use of social media*. [Online]. Available WWW: <http://www.cio.gov/documents> (Accessed 25 June 2020).
- Ferguson-Boucher, K. 2011. Cloud computing: a records and information management perspectives. *IEEE Security and Privacy Magazine* 9(6): 63-66.
- Gatewood, B. 2009. Clouds on the information horizon: how to avoid the storm. *Information Management Journal* 43(4): 32-36.
- Gholami, A. 2016. Security and privacy of sensitive data in cloud computing. [Online]. Available WWW: <https://www.diva-portal.org/smash/get/diva2925669/FULLTEXT01.pdf> (Accessed 14 September 2020).
- Goh, E., Katuu, S., Miller, A., Nordland, L.P. & Sebina, P. 2009. *Module 3: managing the creation, use and disposal of electronic records*. London: IRMT.

- Haradhan, M. 2018. Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People* 7(1): 23-48.
- InformationWeek. 2009. *Government embraces cloud computing*. [Online]. Available WWW: <http://www.informationweek.com/cloud/government-embraces-cloud-computing-launches-app-stored/d/d-id/1083137?> (Accessed 10 June 2020).
- Inland Revenue. 2013. Retention of business records in electronic format, application to store records offshore and application to keep records in Maori. [Online]. Available WWW: <https://www.ird.govt.nz/technicaltax/standard-practice/general/> (Accessed 25 June 2020).
- International Data Corporation. 2014. The digital universe of opportunities: rich data and the increasing value of the internet of things. [Online]. Available WWW: [www.emc.com/collateral/analyst-report/idc-digital-universe-2014.pdf](http://www.emc.com/collateral/analyst-report/idc-digital-universe-2014.pdf) (Accessed 25 June 2020).
- International Records Management Trust. 2004. *The e-records readiness tool*. London: IRMT.
- International Standards Organisation 15489-1. 2016. *International Standard: Information and Documentation – Records Management – Part 1: General*. International Organization for Standardization: Geneva.
- James, R. 2010. Records management in the cloud? Records management is the cloud. *Business Information Review* 27(3): 179-189.
- Jansen, A. 2015. Object-oriented diplomatics. Using archival diplomatics in software application development to support authenticity of digital records. *Records Management Journal* 25(1): 45-55.
- Kable. 2010. Government to use multiple clouds. [Online]. Available WWW: <http://www.kable.co.uk/g-cloud-computing-cio-john-suffolk-22jan10> (Accessed 23 June 2020).
- Kale, A. & Mente, R. 2017. Impact of cloud computing on education system. *International Journal of Electronics, Electrical and Computational System* 6(11): 139-144.
- Kalusopa, T. 2016. Extent of the integration of information communication and technology (ICT) systems in the management of records in labour organisations in Botswana. *Journal of the South African Society of Archivists* 49: 101-115.
- Katuu, S. 2015a. Managing records in South Africa's public sector: a review of literature. *Journal of the South African Society of Archivists* 48: 1-13.
- Katuu, S. 2015b. Managing records in South African public health care institutions. A critical analysis. Unpublished PhD Thesis. University of South Africa. [Online]. Available WWW: <http://hdl.handle.net/10500/19058> (Accessed 12 June 2020).
- Katuu, S. 2016. Managing digital records in a global environment. A review of the landscape of the international standards and best practice guidelines. *The Electronic Library* 34(5): 1-46.
- Katuu, S. & Ngoepe, M. 2015a. Managing digital records in a South African public sector institution. In Anderson, K, Duranti, L and Jaworski et al (eds). *INFUTURE2015: e-Institutions – Openness, Accessibility and Preservation*, Zagreb, Croatia, pp. 135-142. [Online]. Available WWW: <http://doi.10.17234/INFUTURE.2015.16> (Accessed 1 July 2020).
- Katuu, S & Ngoepe, M. 2015b. Managing records created in networked environments within South Africa's legislative framework. In Barbara Endicott Popovsky (ed), *Proceedings of the 3rd International Conference on Cloud Security and Management ICCSM-2015*. Tacoma, University of Washington, pp. 59-70.

- Kentucky State Government. 2012. Cloud computing: implications and Guidelines for Records Management in Kentucky State Government. [Online]. Available WWW: <https://kdla.ky.gov/records/Documents/CloudComputingguidelines> (Accessed 19 July 2020).
- Lewin, K. 2009. Federal cloud computing initiative overview. [Online]. Available WWW: <http://www.scribd.com/doc/18031511/US-Federal-Cloud-Computing-Initiative-Overview-Presentation-GSA> (Accessed 10 June 2020).
- MacNeil, N. 2000. Providing grounds for trust: developing conceptual requirements for the long-term preservation of electronic records. *Archivaria* 50: 52-78.
- McAfee, A. 2009. The cloud future of corporate information technology. [Online]. Available WWW: <http://andrewmcafee.org/2009/08/the-cloudy-future-of-corporate-it/> (Accessed 12 June 2020).
- McLeod, J. 2003. Assessing the impact of ISO 15489 – a preliminary investigation. *Records Management Journal* 13(22): 70-82.
- McLeod, J. & Gormly, B. 2017. Using the cloud for records storage: issues of trust. *Archival Science* 17: 349-370.
- McKemmish, S. 1997. Yesterday, today and tomorrow. A continuum of responsibility. [Online]. Available WWW: <http://www.infotech.monash.edu.au/research/group/rcrg/publications/recordscontinuum-smckp2.html> (Accessed 28 June 2020).
- Miles, M.B., Huberman, A.M & Saldana, J. 2013. *Qualitative data analysis: a method sourcebook*. Thousand Oaks, CA: Sage Publications.
- Miller, R. 2011. Recman adds gmail to cloud records management suite. [Online]. Available WWW: <http://www.fiercecontentmanagement.com/story/recman-adds-gmail-cloud-records-management-suite/2011-08-23> (Accessed 10 June 2020).
- Mosweu, O. 2020. Assessing digital records authenticity in a Botswana government accounting system: an archival diplomatics perspective. *South Africa Journal of Library and Information Science* 86(1): 64-72.
- Mosweu, T. Luthuli, L. & 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. [Online]. Available WWW: <https://doi.org/10.4102/sajim.v21i1.1069> (Accessed 23 June 2020).
- Mugenyi, R. 2018. Adoption of cloud computing services for sustainable development of commercial banks in Uganda. *Global Journal of Computer Science and Technology: B Cloud and Distributed* 18(1): 1-10.
- Mulauzi, F. & Wamundila, S. 2012. The role of records managers in the digital age: the Zambian experience. Proceedings of the Twentieth Standing Conference of East, Central and Southern African Library and Information Associations, 4–8 June 2012, Nairobi, Kenya. [Online]. Available WWW: <http://www.researchgate.net/publication/334397973> (Accessed 28 June 2020).
- National Archives and Records Administration (NARA). 2011. Frequently asked questions about managing federal records in the cloud computing environments. [Online]. Available WWW: <http://www.archives.gov/records-mgmt/faqs/cloud.html> (Accessed 10 June 2020).
- Ngoepe, M. & Saurombe, A. 2016. Provision 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): 22-41.

- Ngulube, P. 2020a. Theory and theorising in information science scholarship. In Ngulube, P. (ed.). *Handbook of research on connecting research methods for information science research* 18-39. Hershey, PA: IGI Global.
- Ngulube, P. 2020b. The movement of mixed methods research and the role of information science professionals. In Ngulube, P. (ed.), *Handbook of research on connecting research methods for information science research*, 425-455. Hershey, PA: IGI Global.
- NSW Government Cloud Policy. 2015. Using cloud computing services: Implications for information and records management. [Online]. Available WWW: <https://www.records.nsw.gov.au/recordkeeping/> (Accessed 19 January 2020).
- Nwabuonu, O.G. & Nwachukwu, N.G. 2014. Cloud computing: a key to IT development in West African sub-region. [Online]. Available WWW: <http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-10/Q0162109498.pdf> (Accessed 3 July 2020).
- Ponemon Institute 2011. Security of cloud computing providers study. [Online]. Available WWW: <http://www.ca.com/-/media/files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf> (Accessed 23 May 2020).
- Queensland Government. 2014. Recordkeeping – general, digital, cloud computing. [Online]. Available WWW: [https://www.health.qld.gov.au/data/assets/pdf\\_file/0032/375809/recordkeeping-infosheet-v2.pdf](https://www.health.qld.gov.au/data/assets/pdf_file/0032/375809/recordkeeping-infosheet-v2.pdf) (Accessed 23 July 2020).
- Reams, B.D., Kuttan, L.J & Strehler, A.E. 1997. *Electronic contracting law*. New York: EDI and Business Transactions.
- Reed, B. 2009. Project 9 report: preservation of Web 2.0 content. Recordkeeping innovation. [Online]. Available WWW: <http://gov2.net.au/files/2009/12/Project-9-Final-Report.doc#Toc248025982> (Accessed 3 July 2020).
- Richards, L.L. 2014. Evidence-as-a-service: state recordkeeping in the cloud. Unpublished PhD Thesis. University of North Carolina. [Online]. Available WWW: <https://www.academia.edu/9098581/> (Accessed 19 January 2020).
- Ross, S. 2000. *Changing trains at Wigan: digital preservation and the future scholarship*. London: NPO Preservation Guidance Occasional Papers.
- Sahandi, R., Alkhalil, A. & Opara-Martins, J. 2013. Cloud computing from SMEs perspective: a survey based investigation. *Journal of Information Technology Management* 24(1): 1-12.
- Saldana, J. & Omasta, M. 2018. *Qualitative research: analysing life*. Los Angeles: Sage Publications.
- Smit, F., Glaudemans, A. & Jonker, R. (eds) 2017. *Archives in liquid times*. GTV: Drukwerk.
- Solanki, G.A. 2012. Welcome to the future of computing: cloud computing and legal issues. *International Journal of Scientific and Technology Research* 1(9): 30-34.
- Spring, C.M. 2011. Reimagine your business. [Online]. Available WWW: <http://www.springcm.com/products/records-management> (Accessed 5 June 2020).
- Stuart, K. & Bromage, D. 2010. Current state of play: records management and the cloud. *Records Management Journal* 20(2): 217-225.
- The Doctrine for the Modernization and Industrialization of Zimbabwe through Education, Science and Technology Development to achieve Vision 2030. 2019. Ministry of Higher and Tertiary Education, Science, Innovation and Technology Development.
- Wang, W.Y. Rashid, A. & Chuang, H. 2011. Toward the trend of cloud computing. *Journal of Electronic Commerce Research* 12(4): 238-242.
- Yakel, E. 2001. The social construction of accountability: radiologists and their recordkeeping. *The Information Society* 17(4): 233-245.

Zimbabwe Open University. 2019. *ZOU Strategic Plan 2019-2023*. Harare: Zimbabwe Open University.