Strategies for preservation of digital records in Masvingo Province of Zimbabwe

by

BLESSED MAGAMA

submitted in accordance with the requirements
for the degree of

MASTER OF INFORMATION SCIENCE

in the subject

ARCHIVAL SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF M NGOEPE

NOVEMBER 2017

ABSTRACT

Information and communication technologies (ICTs) have been embraced by a number of public institutions in Masvingo province of Zimbabwe as part of the government's drive towards e-governance and improved service delivery. This has resulted in the generation of large volumes of digital records that are invaluable for strengthening accountability, transparency, decision making and service delivery. Preservation of these digital records has been cited as a daunting task for most institutions especially in sub-Saharan Africa. The dynamic nature of information technologies, obsolescence issues, as well as media degradation require digital preservation strategies in place to ensure that digital records remain accessible and usable over time. However, the National Archives of Zimbabwe (NAZ) mandated to preserve all types of records is at the moment unable to ingest digital records from public departments for preservation due to lack of adequate digital storage facilities and skilled manpower. The records creating agencies in Masvingo have been left on their own to deal with the digital preservation conundrum yet they are also faced with similar challenges. This qualitative study utilised the Open Archival Information System (OAIS) reference model as the conceptual framework to explore the strategies for preservation of digital records in Masvingo province in Zimbabwe. Data was gathered through interviews with officials from 13 out of 15 public departments that preserved digital records in Masvingo province, augmented by observation and document analysis. Research data was manually processed and thematically analysed in line with the objectives of the study. The study established that the strategies for preservation of digital records in Masvingo province were failing to guarantee their long-term preservation and security due to lack of supportive legislation, standards, policy guidelines, budgets, adequate and conducive infrastructure and skills. This has resulted in swathes of digital memory being lost. The study recommended the adoption of trusted digital repositories (TDRs) that are compliant to the OAIS standard, close co-operation between records creating agencies, NAZ, information technology (IT) experts and the academia in tackling digital preservation challenges, and the development of preservation policies and guidelines, as well as continuous training and provision of budgets to cater for preservation of digital records. In the absence of infrastructure, the NAZ should consider cloud computing for preservation of digital records as an interim solution while observing legal obligations.

Key terms: Digital preservation, digital records, information communication technologies, Masvingo province, trusted digital repositories, Zimbabwe.

ACKNOWLEDGEMENTS

First and foremost, I am very grateful to my supervisor Professor Mpho Ngoepe for his expert advice, guidance, support and patience through-out this research journey. It was through his guidance and mentorship prowess that this project was successfully completed.

I also want to thank heads of government departments, parastatals and the local authority for giving me permission to carry out research in their institutions. The co-operation I got from all the informants cannot go without mentioning. Without them, data collection was bound to fail.

Special thanks also go to the language editor of this project Mr Phineas Chinyanga.

I also extend my gratitude to my wife Ashel Magama and our precious boys Tadiwa Preeminent Magama and Thabo Blessed Junior Magama (Jojola) who stood by me and tolerated me when most of the quality family time was gobbled by commitments along the long and winding journey of this study.

Last but not least, I would like to thank the University of South Africa for sponsoring my studies and the God of my Spiritual Father Apostle Ezekiel Handinawangu Guti for His providence throughout this research journey.

DEDICATION

This dissertation is dedicated to all members of the Magama family for inspiration they gave me during my studies.

Student number: 57664986

DECLARATION

I declare that **Strategies for preservation of digital records in Masvingo province of Zimbabwe** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

07 NOVEMBER 2017

…… **…….....…….……**

SIGNATURE **DATE**

(MR B MAGAMA)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AIP	Archival Information Package
API	Application Programming Interface
CCSDS	Consultative Committee on Space Data Systems
CD	Compact Disc
DAITSS	Dark Archives in the Sunshine State
DIP	Dissemination Information Package
DPC	Digital Preservation Coalition
DRAMBORA	Digital Repository Audit Method Based on Risk Assessment
DSPACE	Digital Signal Processing and Control Engineering
EAD	Encoded Archival Description
E-government	Electronic Government
Email	Electronic mail
ESARBICA	East and Southern Africa Regional Branch of the International Council on Archives
FEDORA	Flexible Extensible Digital Object Repository Architecture
HTML	Hyper Text Markup Language
ICA	International Council on Archives
ICT	Information Communication Technology
InterPARES	International Research on Permanent Authentic Records in Electronic Systems
IRMT	International Records Management Trust
ISO	International Organisation for Standardisation
IT	Information Technology
LOCKSS	Lots of Copies Keeps Stuff Safe
LOD	Linked Open Data
METS	Metadata Encoding and Transmission Standard
NARA	National Archives and Records Administration
NARS	National Archives and Records Services of South Africa
NASR	National Archives of Southern Rhodesia
NAZ	National Archives of Zimbabwe
NESTOR	Network of Expertise in Long-term SToRage
OAIS	Open Archival Information System

PDF	Portable Document Format
PREMIS	Preservation Metadata Implementation Strategy
SIP	Submission Information Package
TB	Terabytes
TDR	Trusted Digital Repository
TRAC	Trusted Repositories Audit and Certification
UK	United Kingdom
UN	United Nations
USB	Universal Serial Bus
XML	Extensible Markup Language

CHAPTER ONE
PUTTING THINGS INTO PERSPECTIVE

1.1 Introduction

Strategies for preservation of digital records are critical to ensure continued access to information. As government services are increasingly executed using Information Communication Technologies (ICTs), the resultant digital records are becoming the basis for confirming pension and other entitlements, registering birth and deaths, verifying citizenship and certifying voting rights, enabling the collection of taxes and census enumeration, supporting financial management and enabling audits and evaluation, helping resolving land claims, supporting litigation, documenting inter-governmental agreements, enabling economic planning, describing the government's accomplishments, documenting its transgressions, monitoring the nation's developments and governance, and enabling countless other information intensive activities (IRMT 2004). As Masuku and Makwanise (2012:179) would attest, digital preservation strategies need to be developed and implemented in order to safeguard records. Failure to implement digital preservation strategies would result in lack of access to archives or records of enduring value which is a blow to human rights activists, auditors, as well as the general populace whose rights are usually abused by those in power.

It is therefore crucial that the created digital records remain reliable, authentic and usable, and have integrity (ISO 15489-1:2001). The guarantee is only through implementing a robust preservation strategy. Kanyengo (2006:5) argues that countries and institutions that are not taking measures today in handling the rapid digital explosion will be left out in accessing knowledge resources that are in digital form when the print form is no longer available to them. This may result in national amnesia and a gap in national heritage due to digital Dark Age (Ngoepe 2017). The importance of effective digital preservation strategies is also increasing as social media and websites are growing as a source of official government and corporate communications. According to Digital Preservation Coalition (DPC) (2016a:1), data on social media platforms is "fast paced and dynamic". There is now urgent need to invest more in scalable trusted digital repositories and technical skills of the staff that will sustain the digital repository (Ngulube 2012:114; Perry 2014:6).

While ICTs enhance access and delivery of government information and services to the public, other government agencies and entities, the hope can easily be futile if a preservation strategy is not put in place to guarantee continued access to large volumes of digital records that are a by-product of e-governance initiatives (Kamatula 2012:41-55; Ngulube 2012:112). According to Cunningham (2011:84), digital information is highly vulnerable to loss through neglect or mismanagement. Ignoring digital preservation challenges for instance, technological obsolescence and fragile storage media, stifles the potential gains society would have received in return for the personal, economic and professional investment in information technology (Adu 2015:58).

This study utilised the Open Archival Information System (OAIS) reference model as the conceptual framework to investigate the strategies for preservation of digital records in Masvingo province in Zimbabwe.

1.2 Contextual setting

Masvingo province comprises seven administrative districts, namely Masvingo, Gutu, Zaka, Bikita, Chiredzi, Mwenezi and Chivi. Masvingo city formally Fort Victoria, is the provincial capital and the oldest town in Zimbabwe. According to the National Archives of Zimbabwe (NAZ n.d), the town came into being on 14 August 1890 when the lumbering pioneer column with its 117 wagons emerged from the providential pass into the comparative safety of the highveld after the dangerous two months trek through the lowveld from South Africa. The town was officially named Nyanda in 1982 soon after independence, but was renamed Masvingo a few months later (NAZ n.d). The town serves as the administrative, commercial and industrial centre for a rich mining and industrial province. Also important to the city's development is its nearness to the Great Zimbabwe ruins or monuments which are a world heritage site of architecturally amazing stone walls from which the country Zimbabwe (house of stones) derived its name. It is also near to Lake Kyle or Mutirikwi, Kyle recreational park and Mushandike national park and sanctuary which attract tourists from all walks of life.

Formal record-keeping in Masvingo province can be traced to the colonial administration which commenced with the granting of the royal charter by the queen of England in 1889 to the British South Africa Company (BSAC) to develop and administer the territory (now Zimbabwe) as a British protectorate (Matangira 2016:23-24). Archival services incorporating

both records and archives management came about with the promulgation of the Archives Act on 12 April 1935 which paved way for the formation of the National Archives of Southern Rhodesia (NASR) on the 1st of September 1935 (NASR 1969: xxxi). With the increase in the volumes of records generated, the 1935 Act was replaced by the 1964 Act as it was making it difficult to pursue a dynamic policy in the management of these records (Matangira 2016). The 1964 Act was also replaced by the 1986 Act because it restricted the National Archives to managing noncurrent records only of conventional paper based materials (Dube 2011:281). The 1986 Act which is in use to date mandates the National Archives to manage all government records from creation to disposition irrespective of format.

It is also clear that by the time of independence in 1980, a lot of investment has been put into the records and archives management business (Matangira 2016:28). Other notable investments included the decentralisation of records centre services to Bulawayo in 1966 to cater for Matabeleland province which was eventually given archival institution status in 2001. Other centres opened as part of the decentralisation of government services after independence include Mutare Records Centre which was opened in 1986 to cater for Manicaland province, Masvingo records centre which was opened in 1987 to cater for Masvingo province, Gweru Records Centre which was opened in 1988 to cater for the Midlands province and Chinhoyi Records Centre which was opened in 1999 to cater for Mashonaland West province. The administration of all these records centres remain largely centralised at the NAZ head-office in Harare to date.

However, the spreading of wings by the national archival institution as well as the improvements brought about by the 1986 NAZ Act did not yield the much anticipated improvements in records and archival management services. The country went through tough political and economic crisis since the dawn of the 21st century and NAZ's records management outreach programmes were negatively affected (Murambiwa 2012). According to Matangira (2016:47), compromised records keeping activities were inevitable as public departments had to operate without the guidance of 'experts' from the NAZ. The period was dubbed a disaster situation by Matangira (2016:47) who further notes that "the momentum that the new government had started off with at independence was beginning to erode and so were record-keeping activities throughout the country". This situation was made worse by the new challenges brought by the generation and dissemination of information using ICTs. Records management systems are steadily changing from primarily paper based administrative systems

to digital systems, thus changing the way information is captured, processed, stored, retrieved, presented and disseminated. This transition is characterised by the production of large volumes of digital records, created and stored in structured databases, unstructured content management systems, social media platforms, web technologies, mobile platforms and on various inherently fragile media (Lemieux 2016:6; Ngulube 2012:114).

Mutsagondo and Chaterera (2014:1) also note that the current archival legislation in Zimbabwe does not adequately provide for the management of these fast proliferating digital records and lacks clear clauses on creation, storage, appraisal, destruction and transfer of digital records to an archival repository. This has resulted in records management practitioners resorting to a hit or miss approach when managing digital records (Mutsagondo and Chaterera 2014). There is no clearly defined strategy on e-government adoption in Zimbabwe (Ruhonde, Owei and Maumbe 2008). The current NAZ Act can be classified as a second generation legislation which according to Parers (2000:7) should be updated, taking into account the electronic environment, convergent technologies, the web environment, web portals and gateways, government online initiatives, transactions, e-business, knowledge and information management amongst other things.

Therefore, NAZ is facing challenges in exercising its mandate of playing a major role in the archiving of digital records. The archival institution is also failing to meet the International Council on Archives' picture of an archival institution in a digital era as outlined in Nkala, Ngulube and Mangena (2012:112) which should:

- Facilitate the establishment of policies, procedures, systems, standards and practices designed to assist the creators of digital records to create and retain records which are authentic, reliable and preservable.
- Be involved in the entire lifecycle of digital records to ensure the capture, preservation and continued accessibility of records identified as having archival value.
- Define the requirements for preservation and accessibility to ensure that digital archival records remain available, accessible and understandable through time.

In practical terms, NAZ at the moment has left the task of managing and preserving digital records to the creating agencies (Bhebhe 2015:118). The NAZ Act does not provide any clue regarding transfer procedures of digital records from registries to the public archives (Mutsagondo and Chaterera 2014:4). No public office in Zimbabwe at the moment has ever

transferred its digital records to the national archival institution (Mutsagondo and Chaterera 2014:4). NAZ at the moment does not have skilled personnel and adequate infrastructure like servers to cater for digital records preservation (Bhebhe 2015). Public departments are managing and preserving digital records according to the systems which best suit their institutions (Nkala, Ngulube and Mangena 2012:114). The NAZ Act also prescribes that records should be transferred to an archival repository after 25 years, but, according to Ngoepe and Saurombe (2016:38), it is practically impossible for creating agencies to wait for such a period to transfer digital records since by that time they might be unreadable or lost.

The accelerated use of ICTs in the country also saw the designing of the Zimbabwe national portal (www.zim.gov.zw) which is hosted by the Zimbabwe Government Internet Service Provider (GISP) whose experience in internet services dates back to 1997 (Chaterera 2012:79). According to Ruhonde, Owei and Maumbe (2008), these developments came about as a result of growing pressure on the public sector to serve citizens electronically following explosive growth in internet usage and rapid development of electronic commerce in the private sector since the 1990s. The government was therefore 'forced' to implement ICT based systems in several departments and ministries (Ruhonde, Owei and Maumbe 2008). The use of the Public Finance Management System (PFMS) to process financial transactions and the Zimbabwe Integrated Performance Management Solution (ZIPMAS) for reporting, evaluating and staff appraisal is clear testimony that digital records are being produced by the government of Zimbabwe (Nkala, Ngulube and Mangena 2012:111). Production of digital records received a boost in Zimbabwe with the launch of the electronic government programme in 2011. According to Mutsagondo and Chaterera (2014:2), this programme aimed at enhancing access to and delivery of government and other services to benefit the citizens, while driving towards effective governance and increased transparency and accountability.

The Ministry of Information and Communications Technology has been developing infrastructure all over the country, as well as setting base stations in remote areas so that every Zimbabwean can benefit from the use of technology. By 2011, fibre optic cables linking Zimbabwe to the rest of the world through South Africa, Zambia and Botswana were laid and duty on ICT products was also removed to promote electronic business (Mambo 2012). Public departments like Zimbabwe Revenue Authority (ZIMRA), Central Vehicle Registry (CVR), Registrar General's department (RG), Zimbabwe Tourism Authority (ZTA), National AIDS Council (NAC), state universities and government hospitals, just to mention a few, are now

generating and storing digital records in their conduct of business alongside their paper records. However, quite a bigger number of public departments in Zimbabwe are still doing business the manual way (Bhebhe 2015:112).

Following the advent of the inclusive government under the Global Political Agreement (GPA), a fully-fledged Ministry of Information Communication and Technology was established. Its mandate includes promoting ICTs to enhance national competitiveness and socio-economic growth, based on the United Nations' electronic government measurement criteria (Comesa 2011 cited in Nkala, Ngulube and Mangena 2012:111). However, Zimbabwe as a nation is at the moment yet to put its ICT policy strategic plan document of 2010 – 2014 into practice (Nkala, Ngulube and Mangena 2012: 99). Bhebhe (2015:114) laments that even if the ICT policy document is put into practice, issues of archiving digital records will still not be addressed, as the draft document is silent about digital records management and preservation. This problem is compounded by lack of provision for management and preservation of digital records in the NAZ Act (Ngoepe and Saurombe 2016).

It is therefore apparent that the execution of ICT based projects in government is done in a piece-meal approach without any policy, strategy or framework of principles to support the creation, maintenance and preservation of digital records and archives (Bhebhe 2015; Nkala, Ngulube and Mangena 2012; Ruhonde, Owei and Maumbe 2008). The problem is compounded by the new type of digital records created on a plethora of social media platforms such as facebook, twitter, YouTube and many others. However, Nduna and Chigodora (2015) note that Zimbabwe has no clear social media policy to guide and govern the use of social media within the public sector. It is in view of the above mentioned circumstances that the researcher felt it relevant to establish how public departments generating digital records in Masvingo under the auspices of the NAZ Act are preserving those of enduring value to guarantee continued access to them.

1.3 Statement of the problem

The main problem this study sought to address is that, public departments in Masvingo province are losing significant digital records that should be strengthening their accountability, transparency and effectiveness in delivering their core mandates. For example, Chaterera (2016:128) finds out that digital records held in public registries in Zimbabwe are not

effectively managed and this directly compromises the attainment of good governance, transparency and effective service delivery. The records are also at risk of misuse, unauthorised alteration and deletion amongst other consequences due to lack of professional guidance in their management (Chaterera 2016:128). The trend has also other negative implications such as depriving future generations of valuable digital documentary heritage. NAZ which is mandated to inspect and examine all public records, give advice concerning their filing, maintenance, preservation and disposal, has at the moment relegated that duty to the records creating agencies due to the absence of supporting policy framework and guidelines, lack of adequate and suitable digital storage facilities, financial resources and skilled personnel in digital archiving (Bhebhe 2015; Ngulube and Tafor 2006; Nkala, Ngulube and Mangena 2012). Digital records were embraced in Masvingo province on top of a chaotic manual paper records system (Maboreke 2007). As Ngulube and Tafor (2006:69) would argue, automating a chaotic records management system creates more chaos that can stifle the preservation of digital information. Consequently, public departments that have embraced digital records in Zimbabwe are grappling much to contain the adverse effects of technological obsolescence (Chaterera 2013:88). Therefore, it is necessary for public departments to come up with sustainable digital preservation strategies and for NAZ to be pro-active and play a leading role in the preservation of digital records.

1.4 Purpose and objectives of the study

The purpose of this study was to examine the strategies for preservation of public digital records in Masvingo province of Zimbabwe with a view to make recommendations for their effective preservation to guarantee their continued accessibility. The specific objectives were to:

i. Identify the strategies the province is using to preserve digital records.
ii. Analyse legal, standards and policy guidelines supporting the preservation of digital records.
iii. Assess infrastructure and resources to cater for the preservation of digital records.
iv. Assess the professional knowledge and skills levels of staff responsible for preservation of digital records.
v. Establish how public departments provide access and security to digital records.
vi. Suggest recommendations for the effective preservation of digital records.

1.5 Research questions

1. What strategies are used to preserve digital records to ensure their continued accessibility?
2. What legal, standards or policy guidelines are in place to support the preservation of digital records?
3. What infrastructure and resources are available to cater for the preservation of digital records?
4. What levels of professional knowledge and skills do staff responsible for preserving digital records possess?
5. How is access and security to the preserved digital records provided?
6. How can preservation of digital records be improved?

1.6 Conceptual framework

Conceptual framework provides an environment where the concepts chosen for investigation are appropriated and become useful to the research problem under investigation (Lester 2005:460). In corroboration of this view, Matangira (2016:53) asserts that conceptual framework provides support to studies by presenting known relationships among variables and sets limits or boundaries for the proposed study. This study used concepts or constructs drawn from the Open Archival Information System (OAIS) model. It was carried out under the notion that digital records need to be preserved in trusted digital repositories that are designed in-line with the OAIS model to guarantee continued access to them.

1.6.1 The OAIS Reference Model

The OAIS model is an international standard that identifies processes and functions common to almost every possible digital preservation environment (Gracy 2008:36). It emerged out of the work of the Consultative Committee on Space Data Systems (CCSDS) in the 1990s (Lowry and Nduna 2015). The CCSDS realised that they had lost a lot of data from their National Aeronautics and Space Administration's early space travels and started to develop a model for an open archival information system which was later accepted as an ISO standard (ISO 14721:2003) (Samuelsson, Oberg and Borglund 2007:3). The model arose to address a situation in which digital data was irretrievably lost (Samuelsson, Oberg and Borglund

2007:3). According to the CCSDS (2012:1), an OAIS is an archive consisting of an organisation which may be part of a larger organisation of people and systems that has accepted the responsibility to preserve information and make it available for a designated community as shown in Figure 1.1.

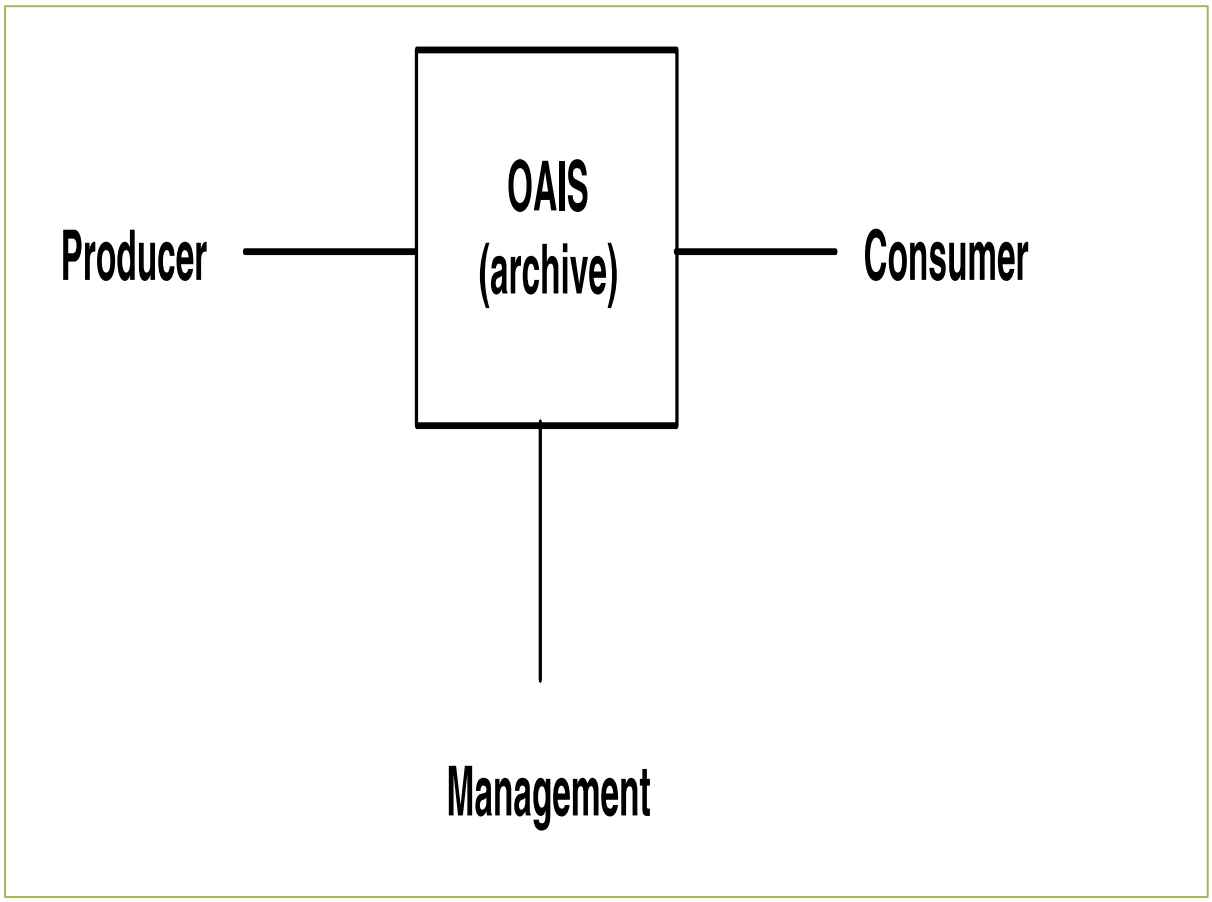


Figure 1.1: The OAIS environment (Lowry and Nduna 2015)

The term ‘open’ is used to imply that this recommendation as well as future related recommendations and standards are developed in open forums and it does not imply that access to the archive is unrestricted (CCSDS 2012). In the OAIS, digital information or objects to be preserved are submitted as Submission Information Packages (SIPs). A SIP is the information package that is transferred from the producer to the OAIS, which will be transformed during ingest into Archival Information Packages (AIPs). An AIP is the information package stored and preserved by the OAIS, which can be made available through Dissemination Information Packages (DIPs) (Hofman 2006:42). A DIP is the version of the information package delivered to the consumer in response to an access request. The information packages contain both the

archived file as well as the descriptive metadata. The functional entities of the OAIS model are further illustrated in Figure 1.2.

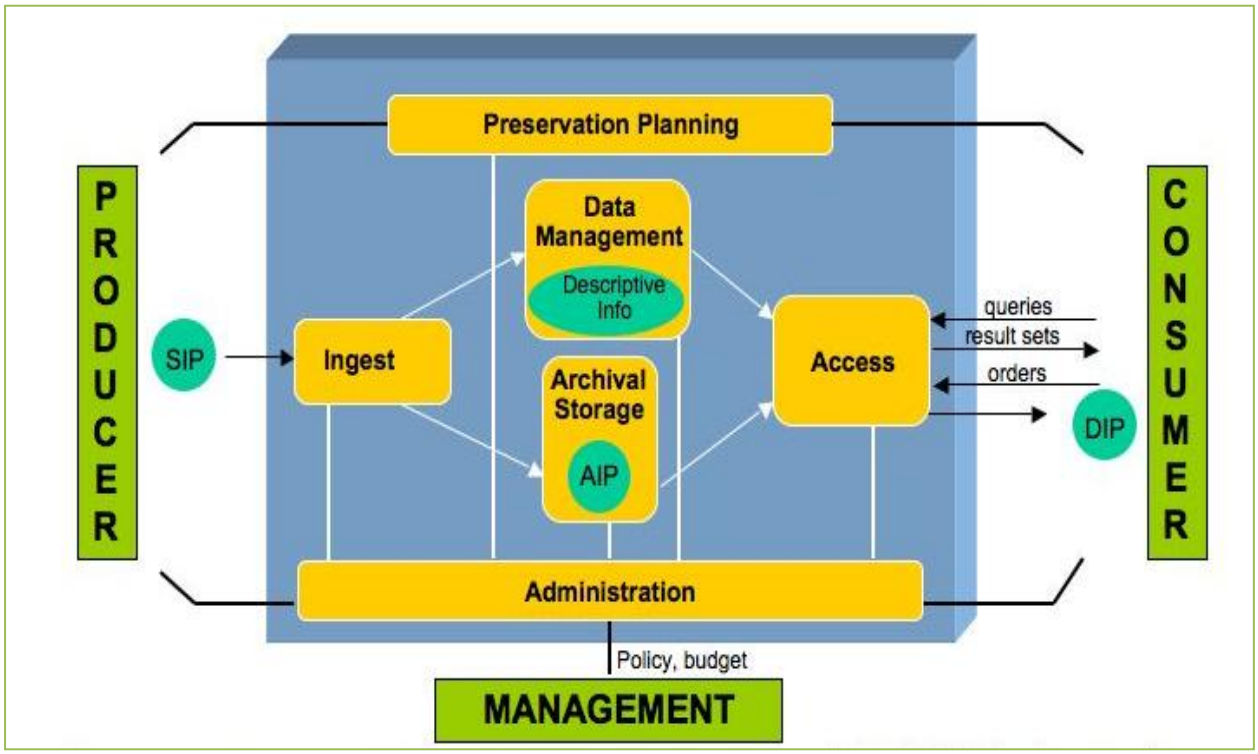


Figure 1.2: The OAIS functional entities (Manojlovich and Bennet 2011)

Below are brief explanations of the six functional entities of the model.

1. **Ingest:** Refers to the set of processes responsible for accepting information submitted by producers (Adu 2015:53). It includes performing quality assurance on SIPs, generating an AIP which complies with the archive data formatting and documentation standards, extracting descriptive information from AIPs for inclusion in the archive database and coordinating updates to archival storage and data management (CCSDS 2012).

2. **Archival storage:** Refers to the portion of the archival system that manages the long-term storage and maintenance of digital material. It also includes receiving AIPs from ingest and adding them to permanent storage, managing the storage hierarchy, refreshing the media on which archive holdings are stored, performing routine and special error checking, providing disaster recovery capabilities and providing AIPs to access to fulfil orders (CCSDS 2012).

3. **Data management:** Maintains databases of descriptive metadata, identifying and describing the archived information in support of the OAIS's finding aids (Adu 2015:53). It administers and updates the archive database functions. It also queries on the data management, generate query responses and produces reports from the query responses (CCSDS 2012).

4. **Access:** Helps the consumer to identify and retrieve information stored in the OAIS. It also includes communicating with consumers to receive requests, applying controls to limit access to specially protected information, coordinating the execution of requests to successful completion, generating responses and delivering the requests to consumers (CCSDS 2012).

5. **Administration:** Manages the day to day operation of the OAIS. It includes soliciting and negotiating submission agreements with producers, as well as auditing submissions to ensure that they meet the archive standards. In addition, it involves maintaining configurations management of system hardware and software. Furthermore, it provides engineering functions to monitor and improve archive operations and to inventory, report on and migrate or update the contents of the archive. Besides establishing and maintaining archive standards and policies, it also provides customer support and activates stored requests (CCSDS 2012).

6. **Preservation planning:** Provides recommendations for conversion, migration, and monitors changes in technology to ensure that the information stored in the OAIS remain accessible to, and understandable by the designated community over the long term, even if the original computing environment becomes obsolete.

1.6.2 Relevance of the OAIS model to this study

This model was found relevant as a conceptual framework to this research because it is almost universally accepted as the "lingua franca of digital preservation" (DPC 2014). It is a common point of reference that is used to build understanding and consensus and to advance the objectives of digital preservation and interoperability. As such, the model has been used as a framework for digital preservation plans, strategies and initiatives around the world and is the

current standard in digital preservation that is considered the benchmark for digital preservation systems (ICA 2016:25; Rogers and Duranti 2012).

The model is invaluable to this study because its functional entities address all aspects of long term preservation of digital information (InterPARES/ICA 2012a:19). Besides providing a framework for the flow of information from the creating agencies to the archive and from the archive to the consumers, the model identifies key processes in systems dedicated to preserve digital information (National Archives of Sweden 2005:42). The emphasis of the model on providing recommendations for conversion and migration, refreshing the media on which archive holdings are stored, extracting descriptive information from AIPs (capturing metadata) and monitoring changes in technology is in line with the first objective of this study that sought to identify the strategies Masvingo province is using to preserve digital records.

The model represents a management framework for receiving, managing and making available digital assets including digital records that need to be retained for the long term (ICA 2016:25). In this regard, the model emphasises on performing routine and special error checking, providing disaster recovery capabilities, identifying and describing the archived information in support of the OAIS finding aids, providing access to fulfil orders, applying controls to limit access to specially protected information and delivering the requests to customers which is in line with the fifth objective of this study that sought to establish how public departments in Masvingo provide access and security to digital records.

The model also advances the notion that, it is important to perform quality assurance on SIPs, generate AIPs that comply with the archive data formatting and documentation standards and maintain the archive standards and policies which is in tandem with the second objective of this study that sought to analyse legal, standards and policy guidelines supporting the preservation of digital records. The model therefore sums up the goal of preservation which is to provide access.

Although there is lack of sufficient standardisation around the OAIS concepts, the model is a foundational resource for understanding and talking about digital preservation (DPC 2014). Furthermore, it is a starting point for implementing digital preservation solutions (DPC 2014). The model provides a framework for describing and comparing different long term preservation strategies and techniques and guides the identification and production of OAIS

related standards (CCSDS 2012:1). According to Asproth (2005:34), standardisation is an important issue for long term preservation of digital records.

Although the model does not specify the method of implementing a digital repository, it establishes a high level framework for understanding the structural organisation of a repository and the most effective way of maintaining content (Knight 2004:1). In addition, the model is useful as a reference model for repository implementers or simply as a checklist for those already in place (Knight 2004:1). Although the high level nature of the OAIS structure and concepts make implementation challenging, all the different communities interested in digital preservation can apply the model in their own particular contexts (National Archives of Sweden 2005:43). The model also provides a framework for assessing and comparing existing archives and their services and functions (National Archives of Sweden 2005:43). All this made the model attractive to be used as a conceptual framework for this study.

1.7 Justification of the study

Available literature has much on assessing digital readiness in the developing world and the benefits of using ICTs in terms of easy generation and distribution of information, promotion of efficiency and effectiveness in service delivery, transparency, accountability, democracy and good governance. However, little attention has been paid on the preservation of the digital records that are by-products of electronic governance. There is paucity of empirical research especially in Zimbabwe in general and Masvingo province in particular on the subject matter. Public departments in Masvingo province are also losing significant digital records that should be strengthening their accountability, transparency and effectiveness in delivering their core mandates. Available literature has little on the preservation of other digital records such as those generated and shared through social media platforms. This has presented a gap for this research to bridge.

Exploring digital preservation strategies is also worthy undertaking bearing in mind that Zimbabwean courts will be expected to accept electronic evidence in line with the Computer Crime and Cyber Crime bill to be presented to parliament soon (Gumbo 2016). There is therefore need for effective strategies for preservation of authentic digital records that are going to support judicial activities. As rightly noted by Mwangi and Wamukoya (2012:99-

100), “unless significant effort is put urgently into digital preservation to secure long term access to these resources, uncertainties over archiving will continue”.

This study has the potential to provide holistic digital preservation solutions with due reference to local administrative context and rationalities, thus giving a thorough understanding and perceptions of the issues involved. This study can also stimulate an increase in the adoption of electronic governance and boost the confidence in the use of ICTs for improved service delivery. This study is a step in the right direction towards mitigating digital preservation challenges, as well as stimulating further researches in digital preservation strategies which are deemed few across sub-Saharan Africa.

1.8 Scope and delimitations of the study

This study focuses on the strategies for preservation of digital records in Masvingo province of Zimbabwe. Key issues under spotlight include the strategies for preserving digital records; legal, standards and policy guidelines; infrastructure and skills requirements; security, privacy and access issues; as well as recommendations that can improve the preservation of digital records in Masvingo province. Public departments scattered in the provincial capital Masvingo, generating and preserving digital records in their conduct of business were targeted to inform this research. NAZ, as well as private sector departments were not part of this study. Top administration officers, records management officers and IT officers were targeted to participate in this study.

1.9 Definition of key terms

The key terms and concepts are explained in this section to provide the context in which they are used in this study.

1.9.1 Digital records

Digital records encompass everything from simple documents composed of plain texts and charts created with word processing and spread-sheet software to complex documents with hyperlinks, motion pictures and or three dimensional images contained both on compact disks or other packages and used in that form (packaged documents) and those accumulated on

servers and used in electronic networks (network documents) (Sugimoto 2008:58). The National Archives and Records Services of South Africa (NARS) (2006:9) define them as, "information generated electronically and stored by means of computer technology". In the NAZ Act of 1986, the definition of digital records is not clear but is presumed to be included in the definition of a record which is stated as "any medium in or on which information is recorded"

According to Ginsberg (2013:4), the United States National Archives and Records Administration (NARA) defines digital records as, "machine readable electronic records whether produced via e-mail, word processing, social media, websites, database or other applications". The term also applies to hard copy materials that are converted into digital copies. Every electronic record whether born digital or converted through digitisation, consists of one or more digital objects or elements such as bits of data that come together to create a word processed document. InterPARES/ICA (2012b:37) define digital records as records created, received and stored in electronic form as the official public records of the public agency in the course of official business transactions by the agency's officers.

For the purpose of this study, digital records are packaged or network documents that are machine readable, comprising of one or more digital elements produced either via e-mail, word processing, social media, websites, database or other applications or hard copy materials that are converted into digital copies through digitisation, created, received and maintained as evidence and information by an organisation or person in pursuance of legal or in the transaction of business.

1.9.2 Digital preservation

Preservation in general is defined by Ngoepe and Van der Walt (2009:2) as "an effort to prolong the useful life of something and avoid its deterioration for as long as possible for future access". This study will focus on digital preservation. According to Perry (2014:1), digital preservation is "the conservation of all digital materials whether they were born digital such as e-mails, websites, video games and other electronic files or whether they have been digitized from analogue materials". According to InterPARES/ICA (2012a:12), digital preservation is the whole of principles, policies, rules and strategies designed to ensure that

digital objects remain accessible, intelligible and usable over time and across technological change, and that their reliability and accuracy is protected, and their authenticity is verifiable.

For the purpose of this study, digital preservation refers to the strategies applied on all digital records in order to maintain and prolong their existence and access across different generations of technology over time and to protect their identity and authenticity.

1.9.3 Trusted digital repository

Trusted digital repository refers to an internationally accepted technologically neutral means of ensuring long term access to digital records and protecting their integrity, completeness, trustworthiness, and above all traceability (Thurston 2012:10). It can also be viewed as a programme or facility that acquires and stores digital objects for preservation and dissemination (InterPARES 3 Project team Canada 2013).

1.10 Research methodology

Methodology is central to the research process because it is the lens through which a researcher looks, when making decisions on acquiring knowledge about social phenomenon and getting answers to research questions (Ngulube 2015). According to Maboreke (2007), research methodology is a systematic way of producing evidence and without it, findings may be dismissed as guess work or common sense that has been made complicated. This study used qualitative research approach and adopted a multiple case study design. Face to face semi-structured interviews were used as the main instrument for data collection. Data was also collected through observation and document analysis to enhance trustworthiness of the findings.

The population of this study comprised of seventy one (71) public departments. Out of these departments, fifteen (15) that preserve digital records in Masvingo province were purposively selected and targeted to inform this study. However, permission was granted in thirteen departments. The participants were also purposively selected and comprised three participants per department drawn from top administration officers, records management personnel and IT officers who were deemed to be involved in the preservation of digital records in their departments. Greater detail on methodology is given and expounded in Chapter Three.

1.11 Ethical considerations

According to Coontz (2008:130), research ethics encompass how research is conducted and whether the researchers have acted responsibly in accordance with scientific norms. This study tried to ensure that the rights of all participants were not violated in any way by adhering to the research values and principles expressed in the 2007 University of South Africa (UNISA) Policy on Research Ethics. This was done without deviating from the objectivity of the study. The overall objective of the study was explained to participants in order to solicit their consent. Participants were assured that the information extracted will be treated confidentially and will solely be used for academic research purpose. The researcher also acknowledged the work of original authors by referencing appropriately. There were no preconceptions or prior values that influenced the results of this study. Greater detail on ethical considerations was dealt with in Chapter Three of this study.

1.13 Structure of the dissertation

This study is divided into six chapters which are as follows:

Chapter One

This is an introductory chapter that covers the background of the study, statement of the problem, purpose and objectives, research questions, justification of the study, scope and delimitations, definition of key terms, ethical considerations and summary of the methodology to address the problem.

Chapter Two

The chapter covers the literature review. Literature was reviewed with the guidance of the research objectives and questions. Possible knowledge gaps were identified to further put the study into focus.

Chapter Three

This chapter looks at the research design and methodology. Key issues expounded include the research approach and design, data collection instruments, population and sampling, data analysis and ethical considerations.

Chapter Four

This chapter analyses and presents the research findings in line with the objectives of the study in an attempt to address the research questions.

Chapter Five

This chapter interprets and discusses the findings presented in Chapter Four. Findings were also compared with those from other related empirical studies where a similar phenomenon was investigated.

Chapter Six

This chapter summarises and concludes the study before making the recommendations to improve the preservation of digital records in Masvingo province.

1.14 Summary

This chapter introduced and provided the background of this study. The chapter highlighted the fact that the use of ICTs and social media in the conduct of business has led to high generation of digital records that are presenting a preservation challenge especially in developing countries like Zimbabwe. This situation is giving justification for researchers to carryout studies like this one in the area of digital preservation. The chapter outlined the purpose and objectives of the study, research questions, and justification of the study, scope and delimitations, definitions of key terms and an insight into the research approach, design and how data was gathered to address the research problem. It also gave the OAIS reference model as the conceptual framework for this study. The chapter reserved extensive methodological explanations to Chapter Three. The chapter also gave a snapshot of the structure of the dissertation showing six chapters each covering a different component. The next chapter presents the literature review.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

Chapter One has provided the introduction and background of the study, and this chapter presented a review of literature. Literature review is a survey of research done in the past about a topic which appraises, encapsulates, compares and contrasts, and correlates various scholarly books, research articles and other relevant sources that are directly related to the current research being undertaken (Kim 2015). It is important in the sense that the value of a topic is brought to the fore when it can be connected to other people's work as "no knowledge exists in a vacuum" (Ngulube 2009:26). According to Wanjohi (2012), literature review helps to:

- Provide a context for the research.
- Justify the research.
- Ensure that the research has not been done.
- Show where the research fits into the existing body of knowledge.
- Enable the researcher to learn from previous theory on the subject.
- Illustrate how the subject has previously been studied.
- Outline gaps in previous researches.
- Show how the current work is adding to the understanding and knowledge of the field.

In this study, literature was reviewed thematically. It involved an examination of published books, journal articles, unpublished masters' dissertations and doctoral theses, conference papers and internet sources on digital records preservation largely in sub-Saharan Africa to further provide the context for this research. The themes were formulated using the research objectives. The following themes guided the literature review:

- Strategies for preservation of digital records.
- Legal, standards and policy guidelines for preservation of digital records.
- Infrastructure and resources for preservation of digital records.
- Professional knowledge and skills.
- Access and security issues.

2.2 Strategies for preservation of digital records

The purpose of this theme or objective was to identify the strategies the province is using to preserve digital records. Digital preservation strategy refers to a coherent set of objectives and methods for maintaining digital components and related information over time, and for reproducing the related authentic records or archival aggregations (InterPARES/ICA 2012a:12). As put across by ICA (2016:46), an effective digital preservation strategy is measured on the basis of:

- Feasibility, that is, the availability of hardware and software capable of supporting the implementation of the strategy.
- Sustainability, that is, its applicability indefinitely into the future.
- Practicality, that is, ability to be implemented within reasonable limits of difficulty and expense.
- Appropriateness, that is, relevancy to the types of records and metadata to be preserved.

Strategies for preservation of digital records are invaluable to address digital preservation challenges such as technological obsolescence, inadequate infrastructure and financial resources, security and privacy issues, paucity of standards, policies and guidelines. Amongst the various digital preservation strategies, this section is going to look at Trusted Digital Repositories (TDRs), refreshing, backup and byte replication, emulation, capturing preservation metadata, encapsulation, migration, normalisation, cloud computing, use of Application Programming Interfaces (APIs) and preservation formats.

2.2.1 Trusted Digital Repositories (TDRs)

Identifying, collecting and storing online publications and organisational records will be a futile exercise if strategies such as developing TDRs are not devised (Ngulube 2012:114). TDRs manage digital resources to their designated community now and in the future and are OAIS compliant. A TDR offers security and can be audited to ensure appropriate performance and quality management (Adu 2015:81). The other qualities of TDRs as outlined by Lowry and Nduna (2015) are that it must:

- Accept responsibility for the long term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users.

- Have an organisational system that supports not only long term viability of the repository but also the digital information for which it has responsibility.
- Demonstrate fiscal responsibility and sustainability.
- Design its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access and security of materials deposited within it.
- Establish methodologies for system evaluation that meet community expectations of trustworthiness.
- Be dependent upon to carry out its long term responsibilities to depositors and users openly and explicitly.
- Have policies, practices and performance that can be audited and measured.

In view of these characteristics, TDRs enhance trustworthiness, which is receiving considerable attention as a preservation strategy (Dobratz, Schoger and Strathmann 2007). This is due to the fact that if the record is not reliable and authentic, there is no need to keep it accessible (Duranti 2010). TDRs therefore, provide a possibility of ensuring long term preservation and accessibility of records and information created and captured by electronic government activities in sub-Saharan Africa (Ngulube 2012). TDRs can be audited and certified through online tools and methodologies. Examples of assessment toolkits include Trusted Repositories Audit and Certification (TRAC), Network of Expertise in Long-term SToRage (NESTOR) and Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) among others. TDRs work well with software tools for digital preservation such as Digital Signal Processing and Control Engineering (DSPACE), Archivematica, Access to Memory (AtoM), Flexible Extensible Digital Object Repository Architecture (FEDORA), Lots of Copies Keep Stuff Safe (LOCKSS), Dark Archives in the Sunshine State (DAITSS), among others. According to Adu (2015:89), these tools are centred on evaluation criteria, a certification process for digital preservation, risk assessment and self-assessment tools and supports metadata standards, systems concepts, selection and appraisal policies and format identification for digital preservation.

2.2.2 Refreshing

It is the process of copying data from one media to another of the same type (Adu 2015:88). It keeps the system infrastructure updated with the most recent technology. Furthermore, refreshing guards against the adverse effects of media corruption or degradation colloquially

called bit-rot (Rinehart, Prud'homme and Hout 2014:30). This strategy may need to be combined with migration when the software or hardware required to read the data is no longer available or is unable to understand the format of the data (Lowry and Nduna 2015). The strategy is necessary because the hardware needed to access and use data is fast changing. Sustainability of the media in the long term should guide the choice of new storage media (National Archives of UK 2014). This strategy has potential to minimise the adverse effects of technological obsolescence.

2.2.3 Backup and byte replication

Byte replication involves creating identical multiple copies of files, file systems or websites and storing them in different locations across many components without the use of specialised software (Adu 2015:85). Data that exists as a single copy in one location is highly vulnerable to software and hardware failure, intentional or accidental alteration and disasters like fire, flooding and so forth. However, Lowry and Nduna (2015) argue that replicated data may introduce difficulties in refreshing, migration, versioning and access control since the data is located in multiple places. Nevertheless, commercial software that supports backup systems allows users to retrieve files backed up at specific points in time. According to Sugimoto (2014) a well-managed and properly executed backup system can restore a document that would have been lost during disasters. The strategy is suitable for short to medium term preservation of digital records (Corrado and Moulaison 2014:4).

2.2.4 Emulation

Emulation is the replicating of functionality of an obsolete system (Lowry and Nduna 2015). It is an approach that uses one computer device or software programme to imitate the behaviours of another device to obtain the same results (IRMT 2009). Emulation is considered a better technique for preserving digital objects that are complex, since some of their information maybe lost during migration to new formats (Ngoepe and Van der Walt 2009:9). Adu (2015:88) also argues that, "emulation operates on the environment of an object, trying to simulate the original environment that the object needs". Though emulation delivers the most authentic possible rendition of a digital object, critics argue that it can be a very complex strategy to implement since it requires not only the preservation of the original objects but also detailed knowledge of the original systems (Barateiro, Antunes, Freitas and Borbinha 2010).

Solely relying on this strategy is tantamount to taking a significant risk as the strategy is anchored by the technical ability of software engineers to emulate a specific environment and sustain it and on the commercial viability of anyone providing such a service (Ngoepe and Van der Walt 2009:10).

2.2.5 Capturing preservation metadata

Metadata is information that characterises another information resource by listing its attributes especially for purposes of identifying, retrieving, managing and preserving that resource (InterPARES 3 Project: Team Canada 2013). Accessibility and usability of content in the digital preservation environment are enhanced through the creation and management of preservation metadata (Corrado and Moulaison 2014). Preservation metadata is in three main categories outlined by Adu (2015:85) as follows:

1. Technical metadata- which gives a description of the physical attributes of digital objects particularly for preservation and rendering.
2. Management or administrative metadata- which establishes the authenticity, rights, ownership and provenance of the digital object.
3. Discovery metadata- which helps to locate, access and use digital content in the long term.

According to Sugimoto (2014), preserving both metadata and digital resources is crucial to any digital archives as the extinction or loss of the metadata can render the resources of a digital archive inaccessible. Available metadata standards or schemas include among others, Preservation Metadata Implementation Strategy (PREMIS); Metadata Encoding and Transmission Standard (METS); Dublin Core Metadata Set; Encoded Archival Context (EAC); e-Government Metadata Standard (E-GMS 3.1) and Encoded Archival Description (EAD).

2.2.6 Encapsulation

This strategy is usually applied to collections that will go unused for long periods of time (Lowry and Nduna 2015). It involves retaining a digital object in its original form as a bit-stream, grouping it along with instructions and whatever else necessary to maintain access to it in the future such as metadata (Thomas 2006). Appropriate types of metadata to encapsulate with a digital object include reference, representation, provenance, fixity and content

information. According to Lowry and Nduna (2015) logical structures called ‘containers’ or ‘wrappers’ are used to provide a relationship between all information components that could be used in future development of emulators, viewers or converters through machine readable specification. The strategy plays a key part in some other preservation strategies (Thomas 2006).

2.2.7 Migration

Migration is the transferring of data to newer system environments and may include conversion of resources from one file format to another or from one old operating system to another so that the resource remains fully accessible and functional (Lowry and Nduna 2015). It is one of the mostly used approaches as it focuses on files and seeks to keep digital objects on current and new media formats (Adu 2015:86). It is useful whenever an operating environment, hardware and software changes. Lowry and Nduna (2015) further argue that migration can be very useful for preserving data stored on external storage media such as Compact Discs (CDs) and Universal Serial Bus (USB) flash drivers among others. However, the strategy is also fraught with the danger of losing or corrupting information (NARS 2006:20). Content functionality or structure may be lost during migration and this often gives authenticity problems. Furthermore, the strategy can also be time consuming, complex and costly for large collections than simple refreshing (Ngoepe and Van der Walt 2009:8).

2.2.8 Normalisation/ Conversion

This strategy involves the migration of digital records to standard formats whereby the data file format is converted to an open format for preservation. The strategy is also referred to as open system computing as it reduces the number of different formats and migration cycles by going straight to an open source format that is always available and accessible (Barateiro, Antunes, Freitas and Borbinha 2010). According to the Joint Technology Committee (2014:14), the strategy promotes interoperability between differing systems, flexibility in upgrading and migration, as well as sustainable access to content. Open standard based formats allow records to be documented and accessible as the normalised version of the digital record is ‘wrapped’ with metadata (Adu 2015). The strategy allows digital objects to be preserved longer in formats bound by accepted standards (Adu 2015:87-88). However some information may be lost during the normalisation process.

2.2.9 Cloud computing

The National Institute of Standards and Technology cited in InterPARES/ICA (2012c:10) defines cloud computing as:

> A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or services provider interaction.

Data is stored in the cloud in known locations with a specific community of consumers who share the same concerns. According to Adu (2015:83), this may be operated by one or more of the organisations in the community, a third party or some combination of them. For many organisations the cloud represents an attractive mode of preserving their digital records. According to Thibodeau (2014) opportunities for using the cloud are as follows:

- Cost savings.
- Reduced pressure on ICT departments to provide the ever increasing storage capacity.
- Access to services outside the normal office environments.
- Better collaboration with geographically dispersed users.
- Potential opportunities for greater automation of record keeping as part of business.
- More time for ICT personnel to devote to other issues where server maintenance and related tasks are lessened.

However, Branco and Santos (2015:4) argue that it is a challenge to figure out how cloud computing can be trusted and provide security level for its full operation. Branco and Santos (2015:4) further argue that there is distrust of users to put data on computers they do not have control over. Therefore, issues of security and guaranteed availability of stored data in an authentic and reliable form are common concerns with cloud computing. Those contemplating moving information and services to the cloud need to adopt a risk based approach in planning which of their records are best suited to the cloud environment (InterPARES/ICA 2012c:8).

2.2.10 Using Application Programming Interfaces (APIs)

Although some of the above strategies such as emulation can be applied in the preservation of social media content, available literature shows that there is need to go an extra mile. Social media is the collective name given to internet based or mobile applications which allow users to form online networks or communities (Hockx-Yu 2014:2). Social media types include social networks, website pages and file sharing or storage. Examples of social networks include Facebook, Google+ and MySpace which are basic social networks and LinkedIn, Yammer among others which are business or professional social networks. Examples of website pages include blogs or micro-blogs such as Blogger, Wordpress and Twitter; Wikis such as, Ballotpedia, Emergency 2.0, Watershed central wiki, Wookieepedia, Brickpedia; and Mashups such as If This Then That and Google Maps. File sharing or storage type include photo library such as Flickr, Picasa and SmugMug; video sharing such as YouTube and document sharing such as Dropbox and Google Docs. The challenge of preserving records on these platforms is that social media files and website pages do not just consist of simple posts, but include embedded files, links, photos, videos and so forth, which need to be addressed in the overall preservation strategy (Ohio 2012:5). As a result, DPC (2016a:7) notes that Web 2.0 content like social media is more effectively preserved through Application Programming Interfaces (APIs)**.**

An API is a kind of backdoor into a social media platform (DPC 2016a). According to DPC (2016a), APIs allow developers to call raw data directly from a social media platform including content and metadata, all transferred together in formats like JavaScript Object Notation (JSON) or eXtensible Markup Language (XML). APIs act as an interface between the social media platform and the consumer of social media data. Data can be harvested directly from platform APIs, or licensing API data from third party resellers, or negotiating an agreement directly with the commercial platform (National Archives and Records Administration (NARA) 2013). Open APIs create customised tools that will allow appropriate export and download.

2.2.11 Using preservation file formats

Not all file formats are supportive of long term preservation of digital records. According to DPC (2016b), archival non-proprietary tried and tested formats that are adaptable to different hardware and software are recommended for use as they minimise the frequency of migration, risk and cost of preservation. Liu (2013) observes that, archival formats can be supported by assigning identifiers and preservation metadata, backup, periodic refreshment and strategic monitoring of format changes. Tasmanian Archive Heritage Office (TAHO) (2015:6-7), gives the following tips on characteristics of file formats for preservation:

- Formats should be open and accessible to avoid loss of control over government owned information due to changes in commercial arrangements. Non-proprietary open standards are usually more fully documented and more likely to be supported by tools for validation than proprietary formats.
- Formats should be of ubiquitous nature. Formats that are in widespread use are more likely to have ongoing and extensive support from software suppliers. In addition, user communities, tools for migration and emulation are more likely to emerge from industry.
- Formats should support the inclusion of metadata which provides vital information on the provenance and technical characteristics of the information.
- Over-specified formats should be avoided. The more complex the format, the more costly it will be to manage and preserve.
- Interoperability is another important consideration when choosing file formats because formats that are supported by a wide range of software or that are platform independent are more desirable.
- Viability is also another important consideration. Formats that provide error detection facilities to allow detection of file corruption which may have occurred during transmission are more recommended.

Table 2.1 gives examples of preservation formats for common file types that according to the State Archives of North Carolina (2012) meet the minimum requirements for long-term retention.

Table 2.1: Examples of preservation file formats (State Archives of North Carolina 2012)

File Type	Suggested Formats
Word processing documents	• Portable Document Format (PDF/A-1a) / (ISO 19005-1: 2005 compliant PDF/A) • Open Document Text (.odt)
Plain text documents	• Plain text (.txt) American Standard Code for Information Interchange (US-ASCII or UTF-8 encoding) • Comma-separated file (.csv) • Tab-delimited file (.txt)
Structured Markup text documents	• Standard Generalised Markup Language (SGML), with Document Type Declaration (DTD) /Schema • Extensible Mark-up Language (XML) (.xml) with DTD/Schema
Spreadsheets	• Open Document Spreadsheet (ISO/IED 26300:2006) (.ods) • Comma-separated file (.csv) • Tab-delimited file (.txt) • PDF/A-1a (.pdf) (ISO 19005-1:2005 compliant PDF/A)
Audio	• Broadcast Wave Format encoded with Linear Pulse Code Modulated (LPCM) (.wav) • Waveform Audio File Format (WAVE) LPCM (.wav)
Video	• Audio-Video Interleaved (AVI) full frame (uncompressed), WAVE Pulse Code Modulated (PCM) (.avi) • Open Media Framework (OMF)
Images	**Raster** • Standard Tagged Image File Format (TIFF) for master copies (non-compression, high resolution) (.tif, .tiff) • Joint Photographic Experts Group (JPEG 2000/ ISO 15444-1p:2004) for safety copies or distribution (.jp2) **Vector** • Scalable Vector Graphics 1.1 (.svg) • AutoCAD Drawing Interchange Format (.dxf)

	• PDF/A-1a (.pdf) (ISO 19005-1:2005 compliant PDF/A)
Databases	• Software Independent Archiving of Rational Databases (SIARD) • Delimited flat file (Plain text) with Data Definition Language (DDL)
Presentations	• Open Document Presentation (ISO/IED 26300:2006) (.odp) • PDF/A-1a (.pdf) (ISO 19005-1:2005 compliant PDF/A) for presentations without animation.
Email	• Microsoft Outlook Personal Storage Table (.pst) which can be converted to XML or PDF/A or Plain text • MBOX
Web pages	• Web Archive (ISO 28500:2009) (.warc, .war) • PDF/A-1a (.pdf) (ISO 19005-1:2005 compliant PDF/A)

Despite the various strategies highlighted above from item 2.2.1 to 2.2.11, scholars like Adu (2015), Ngulube (2012) among others, note that in many African countries there is still much ignorance about online tools and methodologies for digital preservation. Not much has been done to deal with the capture and preservation of government records and publications in an ICT driven environment (Ngulube 2012:115). Akotia (2000) observes that in most sub-Saharan African countries particularly Uganda, ICTs were considered an indispensable tool for enhancing productivity yet little attention was paid to the information management issues and to understand the forces of change that affect the form and integrity of the record created within an IT environment. Cain and Thurston (1998) also note that the Salary Services Bureau (SSB) which is a government department in Zimbabwe responsible for processing civil servants salaries and pensions lost all the information created and stored on computer tapes between 1980 and 1994. The problem came to light when a newly introduced computer based system failed to read most of the computer tapes. This threat of technological obsolescence is further exacerbated by the harsh environmental conditions in sub-Saharan Africa which are not conducive for electronic machines (Asogwa 2012).

According to Ngulube (2012:115), lack of sustainable repository projects in sub-Saharan Africa makes the region fail to guarantee that the continent does not slip into the ‘digital dark ages’. Digital preservation strategies like use of TDRs have not been widely applied. Furthermore, notable works in developing tools and techniques for preserving digital records as

those done by organisations such as the Open Planets Foundation (OPF), Electronic Resource Preservation and Access Network (ERPANET), International Research on Permanent Authentic Records in Electronic Systems (InterPARES), Digital Curation Centre (DCC), Collaboration to Clarify Costs for Curation (4C) and Scalable Preservation Environments (SCAPE) among others are yet to be fully developed in sub-Saharan Africa and Zimbabwe in particular.

Surveys on digital records management and preservation by Lowry (2012), Ngulube (2012), Kalusopa (2011), Mnjama and Wamukoya (2006), Wamukoya and Mutula (2005), Kanyengo (2006), Ngulube and Tafor (2006), Bhebhe (2015), Ngoepe and Keakopa (2011), to mention just but a few mainly in the ESARBICA region where Zimbabwe is an active member, largely looked at capacity challenges in most archival institutions and governments to address issues of digital records management and preservation. There is a dearth of studies and researches across sub-Saharan Africa focusing on preservation of digital records including those proliferating on social media platforms. Within sub-Saharan Africa, Ngulube (2012) observes that there is lack of communication between IT personnel on one hand and archivists and librarians on the other hand, resulting in the designing of systems that do not promote their collective mandate. Consequently, this is rendering most of the repositories in Africa unsustainable (Ngulube (2012)).

2.3 Legal, standards and policy guidelines for preservation of digital records

The purpose of this objective or theme was to analyse legal, standards and policy guidelines supporting the preservation of digital records. The Joint Technology Committee (2014:10) rightly argues that effective preservation of digital records is not an after-thought but requires attention to long-term needs through-out the records life-cycle. In other words, the preservation of digital records is not a stand-alone or a peripheral activity but is embedded within an effective records management programme. Best practices in records management like adhering to legal, standards and policy guidelines are therefore an anchor to effective preservation of digital records.

2.3.1 Legal framework

Legislation has a tremendous impact on how records including those that are created and stored in networked environments are managed in any country (Ngoepe and Saurombe 2016). Legislation provides the essential framework to operate with authority. In many countries legislation relating to the management of records and archives exists in the form of a national archives act (Ngoepe and Saurombe 2016). Legislation also gives clear mandate by establishing detailed practices and procedures for the management of records and archives through-out their life cycle (Ngoepe and Saurombe 2016).

However, existing archival legislations covering the creation, management and preservation of records in sub-Saharan Africa have not kept pace with technology as they cover largely paper records instead of digital records or both (Asogwa 2012; Matangira 2016:84). According to Hamooya, Mulauzi and Njobvu (2011), many countries in southern Africa are operating archives and records management services under out-of-date or incomplete legislation or even without any legislative provision at all. Ngoepe and Saurombe (2016:37) note that Botswana, Namibia and South Africa legislations were written with paper records in mind as they prescribe that records can be transferred from the creating agency to the archives repository after twenty years. The authors further argue that, in a digital environment, creating agencies cannot wait for 20 to 30 years to transfer their digital records as by that time they might be unreadable or lost.

Ndayisaba (2012) describes the Burundi archival legislation as "obsolete". Archival legislation in Ghana also caters for only paper records against the phenomenal growth of digital records (Adu 2015). In addition, internal conflicts in countries like Somalia, Sudan and Congo among others are consuming precious time for developing legislations, strategies and policies for the preservation of digital records (Adu 2015). In the archival legislation of Botswana, the definition of electronic records is not explained (Motupu 2015). Ngoepe (2015) reveals low uptake of cloud storage in South Africa owing to issues such as lake of guidelines and legislation regarding cloud computing.

In Zimbabwe, the current legislation (NAZ Act of 1986) provides for the storage and preservation of public archives and for the declaration and protection of protected historical records and for the matters incidental to or connected with the foregoing. This may be taken to

include the management and preservation of digital records. However a closer scrutiny of the Act especially section 2(a) which defines a public archive as "any public record which is twenty-five years old; and has been specified by the Director as being of enduring or historical value…" shows that the Act was written to cater largely for paper records. As Ngoepe and Saurombe (2016:38) would argue, it is practically impossible for creating agencies to wait for such a period to transfer digital records to an archival repository since by that time they might be unreadable or lost.

The NAZ Act does not adequately provide for the management of digital records apart from merely defining a record as "any medium in or on which information is recorded". According to Mutsagondo and Chaterera (2014:4), the Act lacked clear clauses on creation, storage, appraisal, destruction and transfer of digital records to an archival repository, resulting in records management practitioners resorting to a hit or miss approach when managing digital records. As Matangira (2016:150) also observes, NAZ has not issued any guidelines yet on the management of digital records even though it is mandated to advice and guide the management of public records in any format. In addition, the current legal framework in Zimbabwe is weak in the area of digital records and in particular lacked vibrant guidelines to prescribe day-to-day activities on managing archival materials in digital format (Matangira 2016:150). Digital records management and preservation in most parts of Africa is therefore taking place without stronger supporting legal frameworks. There is a great difference between this African situation with that of developed countries like New Zealand whose Public Records Act of 2005 mandates its national archival institution to ensure long-term preservation of the public sector's digital records, and outlines the requirement for every public office to create and maintain full and accurate records of its affairs (Adu 2015).

2.3.2 Digital preservation standards

Digital records must be stored in trusted digital repositories in accordance with international standards, good practice and in rooms with good environmental controls with much documentation and much regard for their continued accessibility in the face of changing technology (Wamukoya and Lowry 2013:72). The use and development of standards has long been a cornerstone of the information industry. Standards facilitate access, discovery and sharing of digital resources as well as their long term preservation (DPC 2016b). Using standards that are relevant to the digital institutional environment helps with organisational

compliance and interoperability between diverse systems within and beyond the sector (DPC 2016b). Adherence to standards also enables an organisation to be audited and certified. Below are some standards that are deemed useful for digital preservation:

1. **ISO 15489-1:2001- Records Management**

   This standard is according to Lowry and Nduna (2015), the foundation standard which codifies best practices for records management operations. It can be useful for defining the roles, processes and methods for digital preservation implementation. Moreover, the standard's focus is on the long term management of records (DPC 2016b). It also outlines a framework of best practice for managing business records to ensure that they are created and documented throughout their life cycle while remaining authoritative and accessible (DPC 2016b).

2. **ISO 14721:2012- Space Data and Information Transfer Systems- Open Archival Information System (OAIS)- Reference Model**

   The model provides a framework for describing and comparing different long term preservation strategies and techniques (CCSDS 2012:1). Besides providing a systematic framework for understanding and implementing the archival concepts needed for long term digital information preservation and access, the standard is invaluable for describing and comparing architectures and operations of existing and future archives (DPC 2016b).

3. **ISO 31000:2012- Risk Management – Principles and Guidelines**

   This standard provides a framework of principles, and processes for managing risk. It also helps in increasing the likelihood of achieving objectives, improve the identification of opportunities, threats, and effective allocation of resources for risk treatment (Lowry and Nduna 2015).

4. **ISO/IEC 27001:2013- Information Technology- Security Techniques- Information Security Management Systems- Requirements.**

   This standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organisation (Lowry and Nduna 2015). Additionally, it also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. Furthermore, it covers information security leadership, high-level support for

policy, planning an information security management system, risk assessment and treatment. Besides supporting an information security management system and making an information security management system operational, the standard also reviews the system's performance, and corrective action (Lowry and Nduna 2015).

5. **ISO/TR 18492:2005- Long Term Preservation of Electronic Document based Information**

   This standard provides a practical methodology for continued preservation and retrieval of authentic electronic document based information. Furthermore, it includes technology neutral guidance on media renewal, migration, quality, security and environmental control (DPC 2016b). It was developed to ensure authenticity of records beyond the lifetime of original information keeping systems.

However, in the developing world, Lowry (2012:432) cites paucity of standards, policies and guidelines as factors militating against effective digital preservation. Kamatula (2012:41) also notes that, while more documents are created or received electronically by officers in Tanzania through computers, there are no standards and structures to ensure that the records are properly organised and controlled for future access. Full compliance to standards, policies and procedures is also a challenge in many African countries (Matangira 2016:84). Mazikana (2009); Kemoni and Ngulube (2008); World Bank and IRMT (2000); Ngulube and Tafor (2006); Matangira (2016) and also Chaterera, Ngulube and Rodrigues (2014) note the collapse of record keeping systems in the post-colonial period and a general crisis situation in the manner in which records and archives are managed in the ESARBICA region owing to lack of standardisation.

2.3.3 Digital preservation policies and guidelines

A digital preservation policy is an essential foundation for any sustainable digital preservation programme. According to the National Archives of UK (2011:5-6), this policy acts as the authority for those undertaking digital preservation in terms of:

- Articulating roles and responsibilities both within the organisation and many external parties for example contractors, depositors or donors of records.
- Defining a succinct set of success criteria that can be measured against.

- Defining the coverage of the digital preservation activities including the broad categories of records.
- Determining when and how archivists can appraise digital records that will be presented to them for archiving.
- Identifying the presence and owners of a digital preservation strategy.
- Indicating any standards which are to be adhered to in the digital preservation strategy.

The policy also enables digital preservation to be carried out within an agreed framework, and provides a clear line of responsibilities (DPC 2016b). NARA (2013:21) also posits that appropriate preservation policies and retention schedules are a foundation for successful capture and preservation of social media records.

Wamukoya and Mutula (2005) note that at policy level, senior officials and legislators in east and southern Africa are often unaware of the requirements to manage digital records over time so that the evidence base of governments can be secure and accessible when needed by authorised users. Most government departments and archival institutions in the ESARBICA region also lack other supporting policies like ICT, retention and disposal and access in their preservation efforts (Lor 2005). An ICT policy is invaluable for ensuring that institutional information resources and services are well secured using appropriate controls. Furthermore, it ensures that members of the organisation use ICT facilities and services in an appropriate and responsible manner (Lupane State University 2017). On the other hand, an access policy is also critical because it strikes a balance between the right to access information and confidentiality as well as the safety of the record. This in turn ensures compliance with legislation and archival practices thus guaranteeing the existence of digital materials for future users (National Archives of St Kitts and Nevis 2011). As put across by the National Archives of UK (2011), a records retention and disposal policy is also crucial as it prescribes requirements for the length of time a record must be retained and the appropriate means of disposal at the end of its life-cycle.

Ngulube (2005), Kalusopa and Zulu (2009), Kanyengo (2006), and also Keakopa (2010) observe that in sub-Saharan Africa, less attention has been paid to digital preservation policies even though digital records are growing exponentially. Wamukoya and Lowry (2013:70) observe the lack of digital preservation policies in Kenya and Uganda. Botswana also lacks an e-records management policy which makes it difficult to identify, maintain and preserve digital records (Motupu 2015:35). Absence of procedures for the lifecycle management of digital

records is becoming a serious issue across ESARBICA and if not resolved will undermine ICT, electronic government and freedom of information initiatives (Wamukoya and Lowry 2013:71). The amount of digital information has increased geometrically without proper knowledge, strategies, policies and procedures to preserve it (Voutssas 2012). Chaterera (2013) rightly observes that the management of public records in Zimbabwe is an on-going struggle owing to lack of supportive legislation, guidelines, and procedures.

2.4 Infrastructure and resources for preservation of digital records

The purpose of this theme was to assess infrastructure and resources to cater for the preservation of digital records.The intended benefits of e-government are compromised unless there is adequate infrastructure for managing and preserving the digital records that are created (Nkala, Ngulube and Mangena 2012:110). Storing records and archives in appropriate buildings, monitoring and controlling humidity, temperature and sunlight is key to safeguarding records and archives (Ngulube 2003:289). Ngoepe and Van der Walt (2009) also argue that, a good policy and legal framework does not help much if there is no capacity to implement it and sound infrastructure to ingest archival digital records. Available literature shows greater strides in digital preservation infrastructure in countries like Canada and Australia as compared to Africa. According to Library and Archives Canada (LAC) (2008) cited in Ngoepe and Van der Walt (2009:10-11), the Library and Archives of Canada has a unique building dedicated to the preservation and storage of digital records. It includes a village of conservation laboratories made of servers, tape library as well as 48 climate-controlled vaults that house all types of public and private archival records (LAC 2008 cited in Ngoepe and Van der Walt 2009:10-11). The library and archives building of Canada is built from special material to control humidity and temperature (LAC 2008 cited in Ngoepe and Van der Walt (2009:10-11). The National Archives of Australia's digital preservation facilities comprise of a secure and stable environment that houses processing networks, a digital archive and a separate laboratory for staff (Ngoepe and Van der Walt 2009:10-11).

On the contrary, literature also shows that the same cannot be said in the greater part of sub-Saharan Africa. According to Ngulube (2012:112), digital infrastructure in the greater part of Africa is not adequate for capturing, managing and preserving digital records including those on social media platforms. In Tanzania, Lowry (2012:431-432) observes that the National Archives has no facilities for receiving or storing digital records securely. Furthermore, the

ministries and departments creating the digital records also lack the facilities needed to store and preserve them reliably over time. Ngoepe and Van der Walt (2009:10-11), Ngoepe and Saurombe (2016) and Ngoepe (2017) also observe that South Africa lacks infrastructure to ingest digital records into archival custody. South Africa's archival institution has left management and preservation of digital records to creating agencies (Katuu and Ngoepe 2015:136). Nkala, Ngulube and Mangena (2012) and also Mutsagondo and Tsvuura (2015) posit that Zimbabwe is in a similar position to that of South Africa and has in practice left the management and preservation of digital records to creating agencies. Access to electricity and the availability of broadband are additional infrastructural requirements for effective digital archiving (United Nations 2010). However, Keakopa (2008) notes that electrical power cuts are prevalent in African cities like Dar-es-Salaam, Lagos, Gaborone and Johannesburg yet they can cause permanent loss of data. Zimbabwe is also one of the countries with erratic electricity supply.

There are also a number of costs associated with digital preservation like cost of programme and project management, skills training for staff and the new software needed to implement the retention of digital records (Sanett 2013). According to the United Nations (UN 2014:22), Zimbabwe was number 13 amongst the top 20 countries in electronic government readiness rankings in Africa in 2014 which is a category of low level income states. Such a status is very precarious as far as digital preservation is concerned. According to Rinehart, Prud'homme and Huot (2014:33), digital preservation is not a peripheral activity and must be included in strategic planning and allocation of funding. Periodic copying of data, construction and maintenance of data to support old and obsolete data, come with some level of costs which are far and above the budgets of most organisations (Adu 2015:75). However, it is often unfortunate that records and archival programmes are not prioritised in terms of allocation of resources by politicians in the ESARBICA region (Lowry 2012; Wamukoya and Mutula 2005).

2.5 Professional knowledge and skills

The purpose of this objective or theme was to assess the professional knowledge and skills levels of staff responsible for preservation of digital records. Digital preservation is a dynamic and complex profession and as such, it must be adequately resourced by members of staff with appropriate skills (DPC 2016b). Continuous training along modern digital preservation trends ensures that staff members develop, maintain and enhance their digital preservation expertise

(DPC 2016b). According to the Society of American Archivists cited in Perry (2014:6) a modern archivist must be able to:

- Communicate the requirements related to digital archives.
- Formulate strategies needed to organise and preserve them.
- Integrate technologies, tools, software and media within existing functions for appraising, capturing, preserving and providing access to the digital collections.

Lack of these skills has been cited as a teething problem to the African continent in its endeavour to master the concept of digital preservation (Adu 2015:74). Kamatula (2010) and also Egwunyenga (2009) note that records managers and archivists in sub-Saharan Africa lack skills, procedures, standards and practices for handling electronic records and archives in the public sector.

Although efforts have been put in recent years to open training facilities in the ESARBICA region and Africa in general, archival skills in many African countries remained inadequate (Matangira 2016:82). As noted by Wamukoya and Lowry (2013), Kenya, Uganda and Tanzania do have professional archivists as well as training institutions for capacity building but they lack the digital aspect as they focus more on paper records. This study by Wamukoya and Lowry (2013) corroborates the study by Mazikana (2009) who argues that curricula of most archival training institutions in Africa still focus on paper records with very little attention on digital records. Moreover, where digital records exist in the curricula, the learning is just theoretical and lacks the practical elements that widely address issues of actual practice when faced with real life scenarios at the work-place (Mazikana 2009). This is reinforced by Nengomasha (2013:7) who argues that the developments in records and archives training in sub-Saharan Africa have not done much to improve records keeping in organisations. There is therefore fear of losing much digital records. According to Duranti (2010:85), if digital records are not well managed from the point of creation, there may be nothing to preserve at all.

The situation is exacerbated by the brain drain syndrome where professionals leave to the developed world in search for ‘greener pastures’ (IRMT 2011). The other serious challenge is of technophobia particularly among the older employees in most offices in Africa (Adu 2015:74). This is also applicable in the Zimbabwean context. For instance, at Marondera municipality Malemelo, Dube, David and Ngulube (2013:20) observe that computer systems

were not being extensively used in day to day activities and staff members were not well versed with some information technology programmes used in financial records management.

In Tanzania and Kenya, Manyambula (2009) and Kemoni (2007) respectively, establish that most records management personnel in the public sector were undertrained. Similarly, Luyombya and Obbo (2013:24-15) note that land registrars in Uganda were not ICT literate and lacked training and mentorship in using the digitalised system with ease. Ngulube (2012) establishes that much is not known about the software that is used to create and store some of the records on government websites in sub-Saharan Africa. In addition, many software products in this region are developed with built-in proprietary dependencies which may have adverse effects on access and the preservation of websites (Ngulube 2012). This status quo raised interest for this research to investigate the knowledge, technical proficiency and skills of the staff charged with the preservation of digital records in Masvingo province of Zimbabwe.

2.6 Access and security issues

The purpose of this theme was to establish how public departments provide access and security to digital records. Records systems should include and apply controls on access to ensure that the essential characteristics of records, that is, authenticity, integrity, reliability and accessibility are not compromised (ISO 15489-1 2001:10). Authentic documents are those which attest to events that actually took place or information that is true (Duranti 2005). Integrity is related to whether the document can be considered to be complete and uncorrupted during the course of its existence (ISO 15489-1 2001). Reliability reflects to the trustworthiness of a record as a statement of fact established by examining the completeness of the record's form and the amount of control exercised on the process of its creation (Adu 2015). Accessibility or usability refers to the extent to which future end users can view and interact with the preserved data by way of retrieving, presenting and interpreting the data correctly (Mason 2007).

Access, security and privacy controls are crucial for effective and sustainable digital preservation programmes and strategies. According to DPC (2017), rigorous access, security and privacy controls will:

- Ensure compliance with any legal and regulatory requirements.
- Protect digital materials from inadvertent or deliberate changes.

- Provide an audit trail to satisfy accountability requirements.
- Act as a deterrent to potential internal security breaches.
- Protect the authenticity of digital materials.
- Safeguard against theft and loss.

Anyone using the digital preservation system must have appropriate access rights to the stored content (Adu 2015:97). Furthermore, other types of access controls are required for sensitive or confidential content. Appropriate systems for authenticating and authorising users and system access must also be implemented. According to IRMT (2009:25), minimum authentication can be achieved by creating specific operating system user accounts with appropriate permission. On top of that, capturing appropriate audit data for access to and use of a record as part of its metadata is also very crucial (IRMT 2009:25). Access and security issues must be given proper attention because unprotected digital records can be hacked by identity thieves or stolen in bulk (Laudon and Laudon 2005).

The physical infrastructure required to store and manage digital records must also be protected from accidental or deliberate damage. According to IRMT (2009:25), protection mechanisms to the physical infrastructure include:

- Physical access controls.
- Intruder detection systems.
- Fire detection and suppression systems.
- Backup power supplies.

Poor security and confidentiality controls have also been identified as a major factor contributing to the failure in capturing and preservation of digital records in the ESARBICA region (Wamukoya and Mutula 2005:74). According to Ngoepe, Mokoena and Ngulube (2010:51), content, network and personnel security need to be addressed in the digital records management system. Asogwa (2012) also argues that databases containing personal, financial and medical records which are useful to organisations and individuals can pose a threat if proper security protections are not put in place. On another angle, privacy issues surrounding user data further complicates the already complex requirements for selecting and indexing social media content for reuse (DPC 2016a:8).

According to IRMT (2009:25) and also Shinder (2006), the computer system must be protected from:

- Intrusions by external hackers.
- Unauthorised users.
- Unauthorised modification of the stored content.
- Unauthorised copying and distribution of the stored content.
- System failure.
- Technological obsolescence.
- Harsh environmental factors.
- Damage caused by malicious code or other forms of software designed to filtrate or attack a computer system.

Protection mechanisms to computer systems as outlined by IRMT (2009:25) and also Shinder (2006) include:

- Use of password controls.
- Use of electronic signatures.
- Encryption.
- Installing firewalls.
- Use of antivirus software.
- Use of purpose built storage rooms.
- Regular back up of data.
- Assigning a systems administrator.
- Migration.

Security is therefore an important consideration for digital repositories both to guard the collections against malicious damage, loss, forgery and theft and to ensure that files are presented according to user's needs (Gracy and Kahn 2012). Risk assessment, disaster preparedness plans, managing storage media, use of linked open data (LOD) technologies and careful use of social media are some of the ways of addressing access and security issues.

2.6.1 Risk assessment

It is important to assess the risk associated with creating and storing digital records so that priorities can be established for action and so that unforeseen or emergency situations can be dealt with before they become disasters (IRMT 2009:23). Clear and consistent processes must be used to monitor the integrity of the content, context and structure of all digital objects along with their metadata, to search for corruption or other alterations of the data (IRMT 2009:25). Checksums provide a simple and effective means of checking data integrity. The Linux Information Project (2005) defines a checksum as a simple type of redundancy check that is used to detect errors in data. According to IRMT (2009:26), a checksum is created by calculating the binary values (ones and zeros) in a block of data and storing the results with the data and when data is retrieved, a new checksum is calculated and compared with the existing checksum. A non-match demonstrates that the file has been altered in some way. Free tools for generating and comparing checksums include Jstor/Havard Object Validation Environment (JHOVE) and Java checksum (Jacksum).

It is also important to monitor technological change in order to identify potential risks to specific records. Monitoring changes in technology and service allows preservation archivists to maintain high quality and preservation strategies and avoid costly data recovery activities (IRMT 2009:24). Digital repositories must be protected against threats and vulnerabilities such as migration errors, software obsolescence, disk crushes and bit rot. The risk can be minimised through the use of TRAC and DRAMBORA criteria and checklists, refreshing and capturing preservation metadata.

2.6.2 Disaster preparedness

A digital storage system is prone to both natural and human caused disasters. Policies and procedures need to be established to clarify how the records will be stored in the event of a disaster. According to IRMT (2009:30), a disaster preparedness plan must be tested periodically, updated as needed and reviewed carefully in the wake of an actual disaster. A comprehensive disaster preparedness plan as put across by IRMT (2009:30) includes the following elements:

- Detailed instructions for staff to follow in the event of different types and scales of emergency.

- Contact details for key staff and for any emergency services, including specialists in disaster recovery which maybe engaged as contractors.
- Instructions for restoring the content of the digital collection from backup copies.
- A complete description of the hardware and software infrastructure in place to manage the digital objects with enough information to allow the organisation to acquire replacement equipment or new software if required.
- Copies of crucial documentation related to the preservation process, such as operating procedures.

2.6.3 Managing storage media

Records storage media should be stored and handled in accordance with recommended good practices. IRMT (2009:29) outlines the following storage guidelines:

- Media must always be stored in the correct cases, and in their containers when not in use.
- Storage media must not be left in computer drives unnecessarily since prolonged exposure in the computer can cause both heat and mechanical damage.
- Media must not be allowed to come into contact with liquids, dust or smoke, extreme heat and direct sunlight.
- All media types should be stored vertically within a locked fire resistant safe.
- Magnetic media should be kept away from potential sources of magnetic fields including electrical equipment.
- Media that has been stored in climate controlled environments should be left in the operational area for at least 24 hours before they are used. The media need to acclamatise to the changed environment so that it is not adversely affected by the different temperature and relative humidity.
- Computer drives should be maintained and cleaned on a regular basis in order to prevent damage to media.

2.6.4 Linked open data (LOD)

LOD is gradually becoming an important preservation practice for digital archives (Sugimoto 2014). LOD is a way of publishing structured data that allows metadata to be connected and

enriched so that different representations of the same content can be found, and links made between related resources. Zeblith, Fernandez and Rowe (2012), expound that this principle allows every piece of data to be web addressable and linkable. LOD technologies should be available in a common format such as Resource Description Framework (RDF) to allow easy access to existing databases (Adu 2015:98).

2.6.5 Careful use of social media

The North Carolina Department of Cultural Resource (2012) gave the following tips for dealing with social media content:

- There is need to first establish employee boundaries for using any form of social media.
- Social media sites should be established for the agency rather than in the name of an individual employee.
- Use of social media should be consistent with state laws, regulations, policies and IT security policies.
- Agencies should be aware of the terms of service of each social media site.
- Agencies should have both automated content harvesting tools and manual archiving strategies.
- Agencies should maintain a copy of the content from social media sites on a local networked or state owned server.

2.7 Summary

This chapter was devoted to literature review. It articulated on what literature review is and its importance in research. Existing literature on key issues under the spotlight of this research was thematically reviewed guided by the research objectives. This helped to further put this study into context and to identify knowledge gaps that this study intended to bridge. It emerged from the literature that effective preservation of digital records in sub-Saharan Africa is still a mammoth task. Archival institutions and public departments are yet to find lasting solutions to challenges like technological obsolescence, lack of suitable and adequate infrastructure, finances, skills, policies, legal framework, and standards among others. The following chapter looks at research methodology, shedding light on how data was gathered.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

The previous chapter gave a detailed review of literature to provide the context and further justification of this study, as well as showing where it fits into the existing body of knowledge. This chapter looks at research methodology. The chapter is invaluable as it is the premise on which the trustworthiness of the findings of this research is derived. Babbie (2011:482) argues that, interesting findings and conclusions are meaningless to readers if they are not supported by methodological design showing the execution of the study. In other words, "the worth of all scientific findings depends heavily on the manner in which the data was collected and analysed" (Babbie 2011:482). In the same vein, Ngulube (2015) views research methodology as the lens through which a researcher looks when making decisions on acquiring knowledge and getting answers to the research questions. Furthermore, it also specifies the type of research design and method that can be employed to gain knowledge about social phenomenon. Kothari (2004) adds that research methodology gives the methods, the logic behind the methods, and the explanation of why a particular method or technique was used and why other methods were not used. Through this chapter, the researcher is capable of evaluating the research results. This chapter covers the research approach, design, population, sampling procedure, data collection instruments, establishment of rigour of the study, and ethical considerations as illustrated in Figure 3.1.

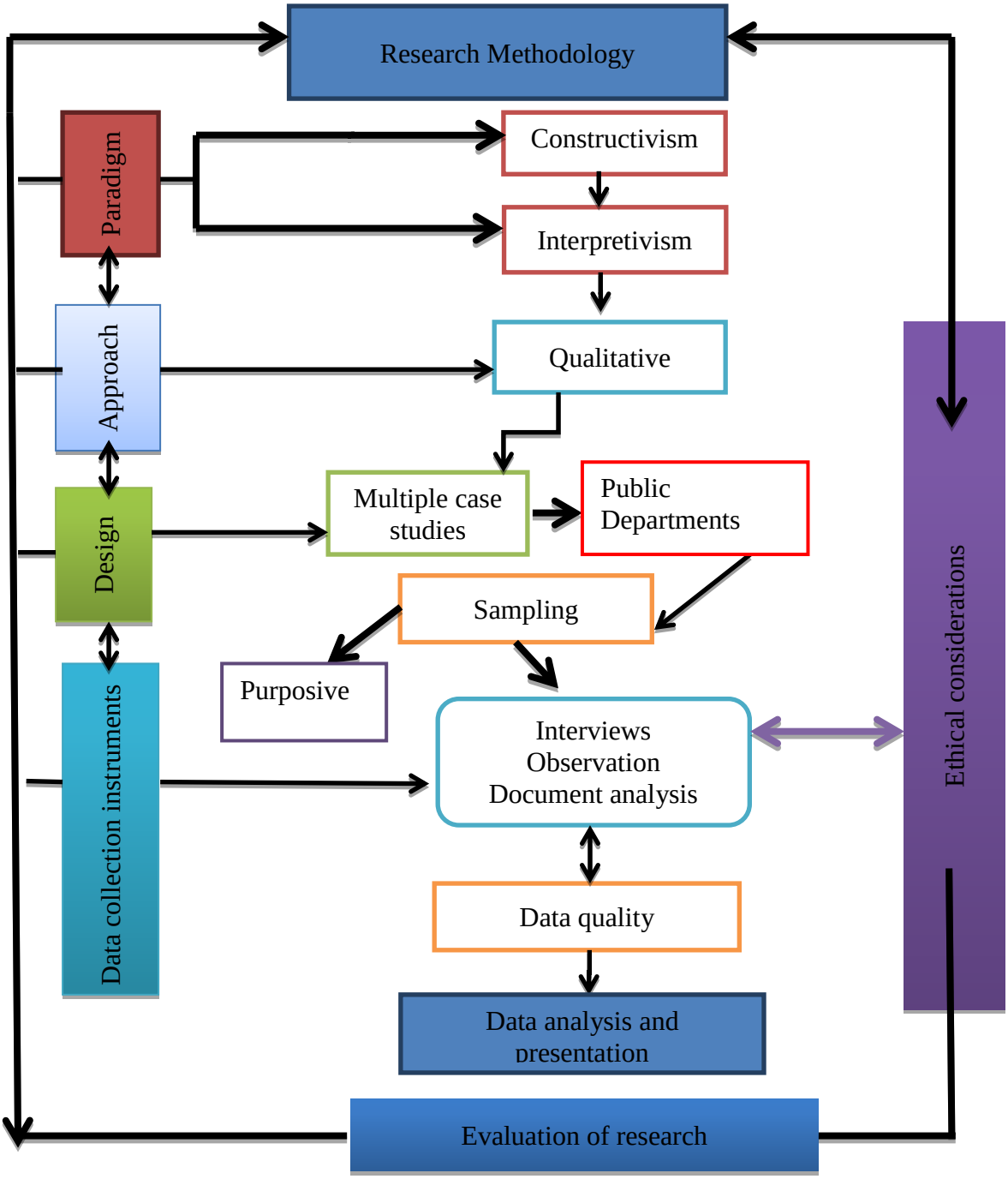


Figure 3.1: Research methodology road map

3.2 Research approach

Research in the social and behavioural sciences has been always premised on two major traditions of research which are quantitative and qualitative research (Tashakkori and Teddlie 2003). Leedy and Ormrod (2005) define quantitative research as an inquiry into an identified problem based on testing a theory, measured with numbers and analysed using statistical

techniques. The approach thrives on statistical and mathematical technique and the philosophical underpinning is realism while the underlying paradigm is largely positivism or scientific (Ngulube 2015). The approach is deductive in nature and tends to be confirmatory. Examples of quantitative research designs include experimentation survey and case study.

On the other hand, qualitative research approach is a broad approach to the study of social phenomenon that is "naturalistic, interpretive, ethnographic and increasingly critical [by] drawing on multiple methods of inquiry (Marshall and Roseman 2006:2). The philosophical underpinning is constructivism while the underlying paradigm is interpretivism (Ngulube 2015). It is concerned with how the social world is interpreted, understood, experienced, constituted, produced and applied (Denzin and Lincoln 2000). The approach is inductive and exploratory in nature. It is based on methods of data generation that are both flexible and sensitive to the social context in which data is produced (Mason 2002:3). Examples of qualitative research designs include ethnography, grounded theory, case study, phenomenological research and narrative research.

Quantitative and qualitative research approaches can be used together depending on the nature of the problem under investigation in what Tashakkori and Teddlie (2010:ix) recognise as, "a third methodological movement" commonly referred to as mixed methods research. According to Ngulube (2010:254), mixed methods research involves collecting, analysing, integrating, and interpreting qualitative and quantitative data concurrently or sequentially in a single study. Additionally, it can also be used in a series of studies investigating the same problem irrespective of which research methodology is dominant, in order to exploit the benefits of combining them to enhance the validity of the findings.

This study used the qualitative approach. As Patton and Cochran (2002) would argue, a qualitative approach aims to answer questions about the 'what', 'how' or 'why' of a phenomenon rather than 'how many' or 'how much' which are answered by quantitative methods. A qualitative approach was considered suffice for this study which aimed at exploring a broader picture of the strategies for preservation of digital records in the public sector departments in Masvingo province. In line with the choice of the qualitative approach in this study Mason (2002:1) argues that:

> Through qualitative research, one can explore a wide array of dimensions of the social world, including the texture and weave of everyday life, the understandings,

> experiences and imaginations of research participants, the ways that social processes, institutions, discourses or relationships work, and the significance of the meanings that they generate.

The qualitative approach was found appropriate for this research since it allows the researcher to use multiple sources of data in order to understand complex social processes in their 'real world context and from the perspective of the participants (Yin 2009; Golafshani 2003). The other reason for using the qualitative approach in this study was that, qualitative data collection methods such as interviews give a true picture of the situation on the ground. Moreover, they use more flexible interactive style of eliciting responses to questions in a more presentable manner (Creswell 2014). Baxter and Jack (2008:544) add that with qualitative approach, the issue or problem to be addressed is not explored through one lens but rather a variety of lenses which allow for multiple facets of the phenomenon to be reviewed and understood. The qualitative approach gives understanding of complex social processes through capturing essential aspects of a phenomenon from the perspective of study participants (Curry, Nembhard and Bradley 2009). Furthermore, it yields non-numerical data that provides depth and detail through description of situations, and observing behaviours in order to generate patterns, themes and ideas (Punch 1998). This explains why the researcher opted for this approach to explore in greater detail the strategies for preservation of digital records in Masvingo province of Zimbabwe through the expressions of the people involved with the preservation of digital records and an assessment of the preservation environment.

Although the qualitative approach was attractive to use in this study, it has got its own limitations. Qualitative research results have been questionable as they are based on personal interpretations and personal opinion (Creswell 2009). Research quality is therefore heavily dependent on the skills of the researcher. Research results can also be easily influenced by the researcher's personal biases and idiosyncrasies (Anderson 2010:1-7). The huge volume of data through the use of multiple sources of data makes analysis and interpretation time consuming (Anderson 2010). However, despite these weaknesses, many studies that sought descriptive data like this current research such as Nengomasha (2009), Matangira (2016) and Mutsagondo (2017) have used qualitative methods because they are able to generate ideas and concepts with in-depth focus and knowledge of the research problem.

3.3 Research design

Research design is a 'blue print' for empirical research, aimed at answering specific research questions (Bhattacherjee 2012:35). It is the logical sequence that connects the empirical data to a study's initial research questions and ultimately to its conclusions (Yin 1994:19). Perry (2000:8) adds that it deals more with the logic of the study than with the logistics and is a plan for moving from the research question to the answer. The quality of any research project is enhanced by a good understanding of the research design (Campbell and Ahrens 1998). According to Sauro (2015), common examples of research designs in qualitative research include:

- Ethnography.
- Phenomenological.
- Case study.
- Narrative.
- Grounded theory.

This study used a multiple case study design to investigate digital preservation strategies in Masvingo province of Zimbabwe. Creswell (1998) refers to a multiple case study design as multi-site study while Baxter and Jack (2008:550) refer to it as collective case study as several cases or events are studied. Yin (1994:13) defines a case study as an empirical enquiry that investigates a contemporary phenomenon within its real life context, especially when the boundaries between phenomenon and context are not clearly evident. In case study research, cases can be individuals, groups, organisations, movements, events or geographical units (Neuman 2003). In this study, the cases were the public departments that preserve digital records in Masvingo.

Case studies are in two broader designs which are single and multiple case studies. A single case study is done to learn about a unique phenomenon which the study focuses on (intrinsic case study), or to provide a general understanding of phenomenon using a particular case (instrumental case study) (Harling 2016:2). A multiple or collective case study is a case study design where several cases or events are studied (Campbell and Ahrens 1998), and is done to provide a general understanding of phenomenon using a number of instrumental case studies that either occur on the same site or come from multiple sites (Harling 2016:2). A single case

study is appropriate in certain conditions while multiple case-study design is better in general conditions (Maki-Turja, Anderson and Huselius 2016).

Although multiple case study design requires extensive resources and time, this research found it relevant because it captures real world context just like a single case design and repeats the procedures on multiple cases (Galloway and Sheridan 1994). This replication enhances the validity and generalisability of the findings. According to Yin (2003) a multiple case study allows the researcher to analyse within each setting and across settings to understand the similarities and differences between cases thereby increasing the robustness of the findings.

The multiple case study design was also found fit for this study where investigations are being made at departments that does not have a common guiding principle for preservation of digital records. Brown (2008:3) also posits that case studies have a distinct advantage of delimiting the study and making it particularistic. The multiple case study design was therefore deemed invaluable to get an in depth understanding and evaluation of the current digital preservation strategies in Masvingo province. The use of case study design in the field of information science has been growing steadily over the years and researchers such as Ngoepe (2008), Nengomasha (2009), Thanye (2014), Moatlhodi (2014), Motupu (2015) among others have also used it.

3.4 Population

Parahoo (1997:218) defines population as the total number of units from which data can be collected such as individuals, artefacts, events or organisations. Babbie (2004) defines it as the entire collection of entities for inferences to be drawn from. It refers to all possible cases of what a researcher is interested in studying (Kothari 2004:10). Welman, Kruger and Mitchell (2005) add that it is a full set of cases from which a sample is taken and is comprised of potential participants to whom the researcher wants to generalize the results of the study. The population for this study comprised of 71 public departments in Masvingo province. The departments were drawn from public sector departments situated in the provincial capital Masvingo, identified from the 2015 list of public departments which constitute the provincial development committee, found at the office of the Minister of State for Provincial Affairs for Masvingo Province. On the list 42 were central government departments, 28 were parastatals and one (1) was a local authority. Before the data collection exercise, the researcher contacted

the departments to find out the ones that preserve digital records. Nine (9) parastatals, five (5) central government departments and one (1) local authority confirmed that they preserve digital records. This gave a total of 15 departments which the researcher purposively chose to participate in this study. These public departments that had begun to preserve digital records were seen as best suited to shed light on the strategies for preservation of digital records in the province. However, the researcher was given permission to carry-out research in 13 departments.

3.5 Sampling procedure

Sampling involves taking a representative selection of the population and using the data collected as research information (Bobbie 2007). Trochim (2006) defines sampling as the process of selecting units for example people or organisations from a population of interest. Furthermore, by studying the sample, we may fairly generalise our results back to the population from which they were taken. Since there is rarely enough time or money to gather information from everyone or everything in a population, the goal becomes finding a representative sample (Chaturvedi 2016:12). However, Creswell (1998:83) warns against choosing a too large sample as this leads to lack of depth as well as choosing a too little sample which makes generalisation impossible.

There are two standard categories of sampling which are probability sampling and non-probability sampling. According to Bobbie (2007) probability sampling is sometimes called random sampling. Probability sampling is a sampling procedure or technique in which the subjects of the population get an equal opportunity to be selected as a representative sample and this probability can be accurately determined (Surbhi 2016). The basis for probability sampling is randomisation or chance. Samples are more representative and have higher external validity. Consequently, when a researcher needs to have a certain level of confidence in the data collection, probability sampling should be used (MacNealy 1999:125). With probability sampling, the samples can be rigorously analysed to determine possible bias and likely error (Henry 1990:17). Examples of probability sampling as outlined by Chaturvedi (2016:10) include:

- Simple random sampling.
- Systematic random sampling.
- Stratified random sampling.

- Multi-stage sampling.
- Multi-phase sampling.
- Cluster sampling.

On the other hand, non-probability sampling refers to any sampling method where some elements of the population have no chance of selection or where the probability of selection cannot be accurately determined (Chaturvedi 2016:17). Non-probability sampling is sometimes called non-random sampling. It involves the selection of elements based on assumptions regarding the population of interest which forms the criteria for selection (Chaturvedi 2016:17). The subjects of the population are chosen arbitrarily to belong to the sample by the researcher. Non-probability sampling is useful for researchers to achieve particular objectives of the research at hand because the sample 'knows' the most or is the most typical (Fink 1995:53). It is much applicable when the research is exploratory. Examples of non-probability sampling as outlined by Chaturvedi (2016:10) include:

- Convenient or accidental or opportunity or grab sampling.
- Purposive or judgemental or expert opinion sampling.
- Quota sampling.
- Snowball sampling.
- Sequential sampling.

After selecting the departments, the researcher went on to select participants through purposive sampling. Purposive sampling is selecting a sample "on the basis of your knowledge of the population, its elements and the nature of the research aims (Babbie 1990:97). In purposive or judgemental sampling, the researchers choose the sample based on who they think would be appropriate for the study. This is used primarily when there is a limited number of people that have expertise in the area being researched (Chaturvedi 2016:43). Purposive sampling was deemed appropriate because not all people in public departments are knowledgeable in records management and preservation.

In this study, three (3) officers from each of the 13 public departments were purposively selected for interviews. These were the top administration officer, the records management officer and the IT officer. However, eight (8) departments had no IT officers at provincial level and this left the sample size for this study at 32 participants. The sample was chosen on the

basis that the respondents have knowledge about the subject of this study and experience with the preservation of digital records in their respective departments. Top management personnel were chosen in their capacity as policy makers and actioning officers who largely depend on preserved records for informed decisions and planning. Records management personnel were also chosen as they oversee the management, preservation and provision of access to the records. IT officers were also chosen as they offer technical assistance and maintenance of the digital preservation infrastructure. Obtaining data from participants with different experiences was an advantage for this study because it prevents information bias, thereby increasing trustworthiness of the information gathered (Sauro 2015). Other studies by Adu (2015), Matangira (2016), Chaterera (2013) to mention just a few also made use of purposive sampling.

3.6 Data collection instruments

Data collection instruments allow researchers to systematically collect information about people, objects and phenomena, and about the settings in which they occur (Elmusharaf 2012). According to Chaleunvong (2009), if data is collected haphazardly, it will be difficult to answer the research question in a conclusive way. As Marshall and Rossman (1999) observe, qualitative researchers usually rely on four methods for collecting information. These are:

- In-depth interviewing.
- Observation.
- Participation.
- Analysing or reviewing documents.

This study used interviews, observation and document analysis as data collection instruments. The use of multiple methods of inquiry is typical of qualitative studies like this one. It is commonly referred to as data triangulation. Baxter and Jack (2008:554) cautioned that the approach often lead to collection of overwhelming amounts of data that require proper management and analysis. More oftenly, researchers find themselves ‘lost’ in the data (Baxter and Jack 2008:554). However, the major attraction to use data triangulation in this study is the fact that the strategy is invaluable for increasing trustworthiness of the findings. Redfern and Norman (1994) outline the advantages of data triangulation as follows:

- Enhances confidence in results.
- Permits validation of instruments and methods (confirmatory purposes).

- Provides a better understanding of the phenomena under investigation (completeness).
- Subdues the naturalistic biases of divergent results.

Therefore, data triangulation technique allows the researcher to thoroughly deal with aspects of a phenomenon under investigation and increases the quantity, quality, validity and credibility of the research data collected (Yin 2003). Similar studies by Keakopa (2007), Chaterera (2013), Moatlhodi (2014), Motupu (2015) and Adu (2015) also used a combination of data collection instruments.

3.6.1 Interviews

Amongst the several research instruments in qualitative data collection, interviews are regarded as one of the widely used and powerful method. Furthermore, interviews enable the researchers to understand the participants and explore their thoughts, experiences and feelings towards the issue under study (Patton 1990; Bryman 2008). According to Begum (2015), qualitative interviews are much more like conversations than formal events with pre-determined response categories. Manson (2002:62) also defines qualitative interviewing or semi-structured interviewing as the interactional exchange of dialogue that may involve one-to-one interactions, larger group interviews or focus group and may take place face to face, or over the telephone or the internet.

Interviews for this research were face to face and semi-structured in order to pursue the same line of questions for all the identified respondents. The researcher was taking notes during interviews. A semi-structured interview is a themed interview guide with few questions that are of a general and open nature. Additionally, it makes the interview more based on flexibility and freedom to ask further questions in response to the replies given by the respondents (Bryman 2008). In the same vein, Kothari (2004) adds that, semi-structured interviews provide similar topics and subject areas to explore and probe. Moreover, they list questions or issues to be explored with a degree of flexibility. This type of interview gives room to alter the sequence of questions and the researcher can engage in probes for more information (Fielding and Thomas 2008:246). In this study, after asking the main question like, “How do you select digital records for preservation?” probes such as “Can you elaborate further on that?” were also posed to gain in-depth information and more complete answers to the question.

Face to face interviews were considered suitable for this current study because peoples' knowledge, views, understandings, interpretations, experiences and interactions are meaningful properties of the reality it seeks to explore. Cohen (2006) argues that semi-structured face to face interviews allow informants the freedom to express their views in their own terms and they can provide reliable and comparable qualitative data. Moreover, they have the highest response rate and permit the longest questionnaire since the interviewer can ask all types of questions and can use extensive probes (Neuman 2000). According to Babbie (2010) probing is a technique involved in interviewing to solicit a more complete answer to a question. It is a non directive phrase or question used to encourage a respondent to elaborate on an answer. In this regard, interviews are therefore a useful way to get large amounts of data quickly (Begum 2015). Detailed information was needed in this study to explore the strategies for preservation of digital records in Masvingo province of Zimbabwe to address the objectives and questions of this study outlined in Chapter One.

However, interviews have their own disadvantages. The major limitation with interviews is that participants may give distorted responses due to personal bias, anger, anxiety, politics and simple lack of awareness (Kothari 2004:99). In other words, interviewees may be unwilling or uncomfortable to share all that the interviewer hopes to explore (Marshall and Rossman 1999). The appearance, tone, voice, question wording and so forth of the interviewer may affect the interviewee. Neuman (2000:273) also argues that high costs and time consuming are the biggest disadvantages of face to face interviews. However, despite these limitations, interviews can go further to investigate motives, perceptions and feelings. Moreover, interviews minimise some challenges like, low response rate, reporting error, completion by a wrong person and lack of control over how the respondents interpret questions (Bernard 2000:233).

3.6.2 Observation

Yin (2009) defines observation as a way of gathering data by watching behaviour, events or noting physical characteristics in their natural settings. It is the gathering of primary data by the researcher's actual observation of pertinent people, actions and state of affairs without inquiring from participants (Motupu 2015:66). It relies on first-hand and eye-witness experiences of places, activities and events. Manson (2002) argues that not all knowledge is articulable, recountable or constructible in an interview. Observation allows the generation of multi-dimensional data on social interaction in specific contexts as it occurs, rather than relying

on people's retrospective accounts, and their ability to verbalise and reconstruct a version of interactions or settings (Manson 2002:85-86; Nachimias and Nachimias 1996). Knowledge generated through high quality observation is usually rich, rounded, local and specific (Manson 2002:89).

According to Trochim (1999) there are two types of observation which are participant observation and non-participant observation. Participant observation requires that the researcher becomes a participant in the culture and context being observed (Trochim (1999). This type of observation provides certain unusual opportunities for collecting case study data by gaining access to events or groups that are otherwise inaccessible to scientific investigation (Yin 1994). Begum (2015) adds that in participant observation, the researcher is able to perceive reality from the viewpoint of someone 'inside' the case study rather than external to it. However, the major weakness of participant observation is that the investigator has less ability to work as an external observer and may have to assume positions of advocacy roles contrary to interests of good scientific practices (Begum 2015:48).

On the other hand, non-participant observation is where the observer watches the situation openly or concealed but does not participate (Trochim 1999; Elmusheraf 2012; Urquhart 2015). This type of observation is suitable for investigating phenomena that researchers can observe directly (Nachimias and Nachimias 1996). This is the type of observation that was used in this study. The following were observed in departments during data collection on strategies for preservation of digital records in Masvingo province of Zimbabwe:

- Digital preservation strategies and procedures.
- ICT equipment.
- Personnel involved in digital preservation processes.
- Digital records preservation systems.
- Types and classes of records preserved.
- Digital preservation environment.

According to Hancock, Ockleford and Windridge (2009:18), non-participant observation enables the researcher to see how people actually behave as opposed to what they claim to do in interviews which may not be true. This type of observation does not rely on people's willingness to provide information (Hancock, Ockleford and Windridge 2009). Furthermore, this observation gives additional and more accurate information on phenomena being studied.

As explained by Urquhart (2015), non-participant observation is useful, feasible and can be combined with other types of data collection. In this research, observation data was fused well with interviews and document analysis to increase the rigour and trustworthiness of research findings. According to Oates (2006:202), this is very important to minimise respondent bias. The choice of this type of observation was also influenced by the fact that the researcher had limited time and resources for him to serve attachment periods in the thirteen (13) departments investigated for the purpose of experiencing how each department preserve digital records. The researcher jotted down observation data in his note book during the observation sessions.

Like any other data collection instrument, observation has its own limitations. Olsen (2012) argues that observation is susceptible to subjective bias on the part of the researcher. According to Yin (1994), time consuming, selectivity and reflexivity are the weaknesses of the observation method. Kothari (2004) also notes that observation does not increase the researcher's understanding of why people behave the way they do and issues concerning infringement of confidentiality or privacy may arise. Fully aware of such limitations, observation was used along-side interviews and document analysis. The researcher sought permission in writing, to carryout observations in each department well in advance. The research topic, aim, as well as issues of confidentiality were clearly explained in the letters for seeking permission to carry out research in the targeted departments.

3.6.3 Document analysis

Document analysis involves the procedures used in analysing and interpreting data generated from documents and records (Schwandt 2007). It is sometimes referred to as data mining (Begum 2015). In this study, document review was used to complement data obtained through interviews and observation. This is in line with Patton (2002:294) who notes that documents generate ideas for questions that can be pursued through interviewing and observation.
In this study, the following documents were reviewed:

- Preservation policy or guidelines.
- Retention and disposal policy or guidelines.
- Guidelines for handling storage media.
- Repository audit checklist.
- ICT policy.
- Access policy.

- Disaster management plans.

The major attraction for using document analysis in this study was the fact that documents constitute a rich source of information about an organisation and they also comprise written material about activities carried out within it (Patton 2002). According to Schram (2003), they contain thoughtful data because adequate time and care is given to compile them. Documents are therefore a good source of background information. Well-kept documents are also less likely to be subject to memory decay or distortion compared to data obtained from an interview (Yin 2009). Finn and Jacobson (2008) also argue that the method is relatively inexpensive and may bring up issues noted through other data collection instruments.

However, like any other method, document analysis has its own share of weaknesses. Yin (2009) argues that there are chances of bias in the documents because of the selective survival of information and the fact that documents may contain incomplete and inaccurate information or may lack detail.

3.7 Establishing rigour of the study

Rigour involves issues of accuracy, reliability and validity (Matangira 2016:106). In qualitative research validity and reliability are often referred to as trustworthiness and credibility (Creswell 2014). Positivists often question the trustworthiness of qualitative research, arguing that validity and reliability cannot be addressed in the same way in naturalistic work (Shenton 2004:63). However, many writers like Silverman (2001) and also Guba (1981) have demonstrated that qualitative research can incorporate measures that deal with validity and reliability. According to Guba (1981); Golafshani (2003) and also Billups (2014:1), rigour in qualitative research can be attained by considering four constructs of trustworthiness which are:

- Credibility.
- Transferability.
- Dependability.
- Confirmability.

Credibility is ensuring that the findings are believable, truthful and capture a holistic representation of the phenomena under exploration (Billups 2014). In this study, credibility

was attained through the use of different data collection methods and different types of informants. This is commonly referred to as triangulation and the practice is recommended by scholars like Yin (2009) and also Creswell (2014). Using multiple data sources produces greater depth and breadth of information about the phenomenon under investigation. It helps to corroborate findings and to build a more holistic picture of the phenomenon (Billups 2014:2). This study combined data obtained through interviews, observation and document analysis. Using multiple data collection methods gives rigour to the study through building on the strength of each data collection method while minimising the weaknesses of a single approach (Matangira 2016:107). Credibility was also attained through soliciting data from different participants, that is, top management personnel, records management officers and IT officers.

The research instruments were pre-tested to detect flaws in data collection and to enable the researcher to refine them as recommended by Yin (2009). Pre-testing ensures that data collected from respondents will not give ambiguous statements, but can be relied on. In this study, the researcher sent to the supervisor the first draft of the interview guide for review. The feedback and remarks from the supervisor offered the researcher the opportunity to fine tune the research instrument so that it can yield credible data. After that, interview questions were posed to officers at the Zimbabwe Tourism Authority department in a pilot study. The pilot study gave the researcher insight into the need to explain technical terms, make clearer some vague questions and remove repeated questions. According to Adu (2015:138), pre-testing is invaluable for data collection instruments to pass the test of reliability, validity, consistency, dependability and replicability of the data.

Rigour in this study was also established through ensuring that the findings are stable, consistent and comparable in-line with the dependability and transferability constructs of trustworthiness. The focus was on producing findings that other researchers can interpret for similar settings even to the extent of applying the research design for their own purposes. This was achieved through carefully planning the data collection process, and giving extensive detail and explicit descriptions when recording conversations, observation and interpretations during data collection as recommended by Shenton (2004:73).

Rigour was again established through ensuring that the findings are accurate so as to generate confidence and to reflect the truthfulness of the participants' perspectives. This is in-line with the confirmability construct of trustworthiness. According to Billups (2014:4), confirmability

articulates the extent the researcher worked to neutralise his or her own bias, motivation or interest in the reporting of findings. To eliminate participants' biases, the researcher did the following, as recommended by Chaleunvong (2009):

- Eliminated vaguely phrased questions after pre-testing the data collection instruments.
- Avoided leading questions that cause the respondent to believe that one answer will be preferred over the other.
- Arranged questions in a logical order.

To minimise investigator bias, the researcher used a well prepared observation checklist with a list of specific 'objects' to be observed as recommended by Chaleunvong (2009). Interview biases due to mistrust by the interviewees were reduced in the following ways as also recommended by Chaleunvong (2009):

- Adequately introducing the purpose of the study to the informants.
- Phrasing questions on sensitive issues in a positive way.
- Taking sufficient time for the interviews.
- Assuring informants that the data collected will be confidential.

3.8 Ethical considerations

As earlier on alluded to in Chapter One, research ethics encompass how research is conducted and whether the researcher has acted responsibly in accordance with scientific norms (Coontz 2008:130). Research ethics minimise the risk of abuse or making mistakes which are of real consequence to the people under study. According to Creswell (2009), it is therefore important for researchers to protect their participants, develop trust with them, promote the integrity of research, and guard against misconduct and impropriety. Ethical considerations are very critical to avoid physical or emotional harm which according to Chaleunvong (2009) can be caused by:

- Violating informants' right to privacy by posing sensitive questions or gaining access to records which may contain personal data.
- Observing the behaviour of the informants without their knowledge.
- Allowing personal information to be made public which informants would want to be kept private.

- Failing to observe or respect certain cultural values and traditions or taboos valued by the participants.

To deal with these issues, the researcher adhered to the values and principles expressed in the 2007 University of South Africa (UNISA) Policy on Research Ethics. The researcher sought permission in writing to carryout research in each department, explaining clearly the research topic and purpose of the study. The researcher also ensured that the rights of all participants were not violated by obtaining informed consent from participants before the actual data collection exercise. The researcher agreed with the participants on dates for data collection through interviews, observation and document analysis and the schedule was strictly followed. This is in-line with the recommendation of Olsen (2012) and also Yin (2009) who argue that the basic ethical issues in social science research include issues of informed consent by participants, the respect of their privacy and the safeguarding of the confidentiality of the data. As elaborated by Matangira (2016:113), informed consent is a mechanism for ensuring that people understand what it means to participate in a particular research study so that they can decide in a conscious and deliberate way whether they want to participate.

The researcher established good relationship with the informants to gain their trust. The ethical clearance certificate obtained from the university helped in this regard as well as regular visits to the departments. According to Chaleunvong (2009), this is really critical if the research involves exploring sensitive issues. Regularly visiting departments gave the researcher an opportunity to learn some of their organisational culture so as to better appreciate and understand their concerns and perspectives during the actual data collection sessions. The researcher also made an effort to create a friendly atmosphere so that respondents can feel at ease during interviews.

The researcher also ensured the confidentiality of the data collected. Participants were told that their names were not going to be mentioned in the collected data. Furthermore, the studied departments were assigned alphabetical letters A to M to ensure anonymity. The information gathered was treated confidentially and was solely used for academic research purpose. The researcher also acknowledged the work of original authors by referencing appropriately. No preconceptions or prior values shaped the results of this study. In addition, the results of the study were not falsified or exaggerated.

3.9 Evaluation of research methodology

This study used the qualitative research method to address the research problem. Interviews, observation and document analysis were preferred and used in this exploratory study over questionnaires as data collection instruments. However, the methodology presented some challenges to the researcher. Firstly, there was a lot of ground work done before the actual data collection exercise. This included seeking approval or permission to conduct research from heads of departments, seeking the consent of participants, and making appointments with them for interviews. This made the research process time consuming. The researcher became patient and persisted in visiting the departments several times to explain the objectives of the study and to assure participants and heads of departments that the collected data would be kept confidential and used for academic purposes only. In some few departments, the researcher was referred to get permission to conduct research from their head offices in Harare. This was done though it added more expenses to the research budget. Secondly, the researcher experienced challenges in getting some of the copies needed for document analysis from some participants. However, this did not affect the trustworthiness of the findings of this study much. The researcher used document analysis together with interviews and observation. This data triangulation together with pre-testing of the research instruments helped in strengthening the trustworthiness of the research findings.

3.10 Summary

This chapter covered the methodology of this study. The study took the qualitative approach in the form of a multiple case study design. The research used interviews, observation and document review as data collection instruments. Fifteen (15) public departments that preserve digital records in Masvingo were targeted as units of analysis for this study although the researcher managed to get clearance to carry-out the study in 13 departments. Interviews were carried out with thirty-two participants comprised of top management officers, registry personnel, as well as IT officers. Triangulation of data through the use of multiple methods of inquiry and different kinds of informants as well as pre-testing of data collection instruments were the major ways through which the researcher established rigour of this study. The chapter also looked at research ethics which are critical to protect participants, develop trust with them, promote integrity of the research findings and guard against misconduct and impropriety. The next chapter looks at data analysis and presentation of research findings.

CHAPTER FOUR
DATA ANALYSIS AND PRESENTATION

4.1 Introduction

The previous chapter elaborated on the methodology that was used to obtain data for this study. This chapter deals with the analysis procedure and presentation of data. The chapter is important as it presents data in an intelligible and interpretable form in order to identify trends and relations in accordance with the research objectives (Vosloo 2014). Analysis and presentation of data is critical in any study because the findings provide the foundation for the overall conclusions and implications of the study (Harding University 2017). Investigated departments were assigned alphabetical code letters ranging from A to M and names of interviewees were not publicised for anonymity. Data presentation took the form of descriptive text and tables. Data collected through interviews, observation and document analysis was integrated and presented in line with the objectives of the study to address the research questions along the following sub-headings:

- Digital records preservation in Masvingo province.
- Legal, standards and policy guidelines.
- Infrastructure, resources and tools for digital preservation.
- Professional knowledge and skills levels of staff.
- Access, security and privacy issues.
- Recommendations and suggestion.

4.2 Data analysis

Data analysis involves "creating categories, indexing or coding documents, sorting data to locate patterns, describing patterns, generating theories from data and validating the theories (Blaikie 2010:26). In simpler terms it refers to the procedures followed in interpreting and presenting data (Creswell 2009:151). It is a process of bringing order, structure and meaning to the mass of collected data. Data analysis is considered to be the important step and heart of the research in research work because it transforms raw data into information by arranging it in a certain format or a meaningful order (Tiwari 2013). Furthermore, data analysis and interpretation are the most critical and essential supporting pillars of research (Tiwari 2013:126). Qualitative data analysis is usually based on three stages that is, preparing and

organising data; coding the data; and presenting the data in the form of text, tables and figures (Adu 2015:147). Qualitative data analysis methods include among others:

- Comparative methods.
- Discourse analysis.
- Content analysis.
- Narrative analysis.

In this research, data was manually processed and analysed using thematic content analysis. Content analysis is probably the most prevalent approach to the qualitative analysis of documents and it comprises a searching out of underlying themes in the materials being analysed (Bryman 2004:392). According to Miles and Huberman (1994:11), content analysis is "a form of analysis that sharpens, sorts, focuses, discards and organises data in such a way that 'final' conclusions can be drawn and verified". It allows categories to emerge out of data and recognises the significance for understanding the meaning of the context in which an item being analysed and the categories derived from it appeared (Bryman 2004:542). By using the category system, the aspects which are to be filtered from the material are defined. The strength of content analysis is that the material is analysed step-by-step (Bryman 2004). In line with Creswell (2009:185)'s outline of stages followed in content analysis, the researcher:

- Put together raw data.
- Organised and prepared the data for analysis.
- Read through all data.
- Coded the data.
- Came up with themes.
- Interpreted themes.
- Drew conclusions from the themes.

The research objectives formed the basis of the themes and were used as categories of analysis. Through coding, the researcher was able to reduce and integrate raw data into a small number of classes which contain information required for analysis. Themes in each case called within case analysis were noted first and this became be the first level of analysis. The within case analysis was followed by thematic analysis across cases referred to by Creswell (1998) and also Yin (2003) as "cross case analysis or synthesis", before conclusions were deduced and this

became the second level of analysis. Figure 4.1 summarises the data analysis procedure used in this study.

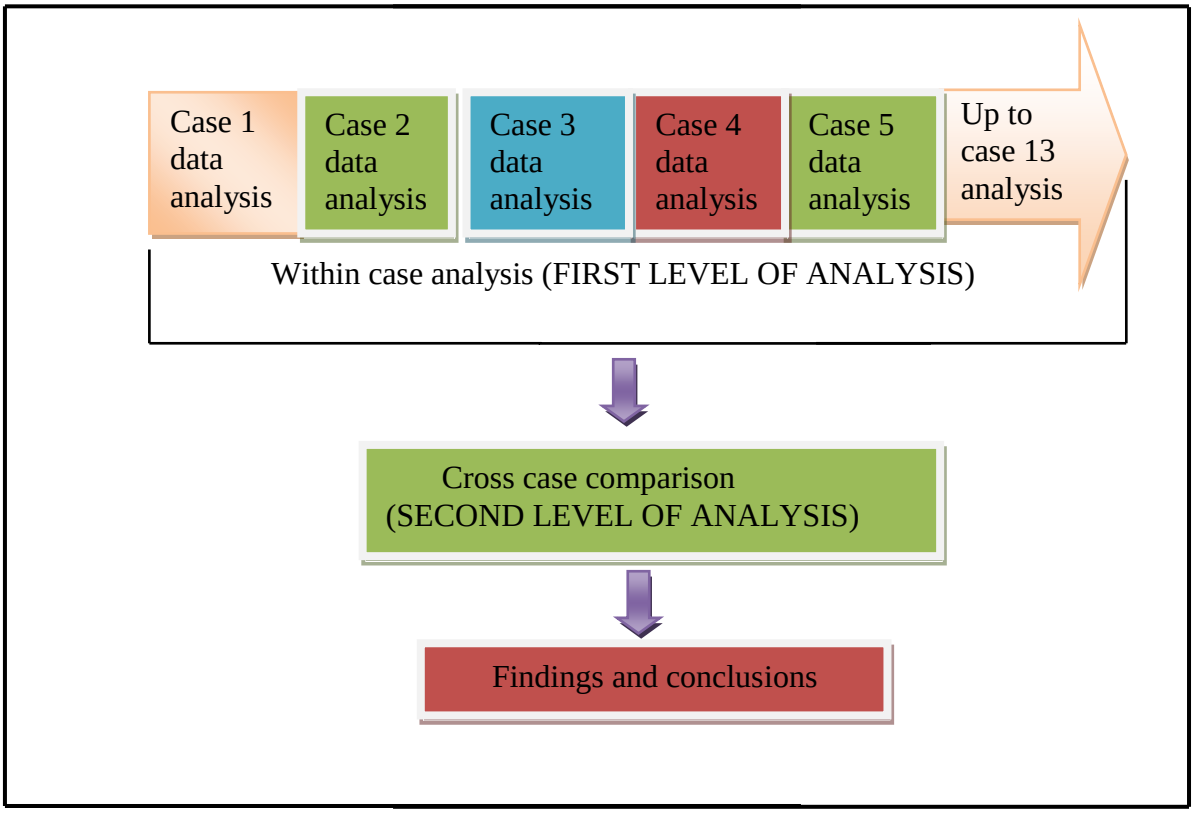


Figure 4.1: Data analysis procedure

4.3 Digital records preservation in Masvingo province

The first objective was to establish the strategies used in Masvingo Province to preserve digital records. Before getting into the strategies, the researcher found it prudent to establish when the studied departments started preserving digital records, the classes and file types they preserve, how they select digital records for preservation and how they ingest the selected digital records into their archival custody. In support of that, ICA (2016) posits that any digital preservation strategy must be appropriate and relevant to the types of records and metadata to be preserved.

4.3.1 Beginning of digital preservation in case study departments

This study established that departments in Masvingo province started preserving digital records at different times as illustrated in Table 4.1. The decision by departments to preserve their digital records was slow and gradual. One department started preserving digital records 20 years ago and the recent ones started four years ago. The general expression in the departments that started preserving digital records after 2010 can be summarised in the view of the registry officer at department I who said, "As a department we could have started preserving digital records earlier but our challenges were lack of skills, equipment, resources and legal framework to do that and we are still grappling with these challenges". All the studied departments also highlighted that they were running hybrid systems of both paper and digital records. The records management officer at department E reinforced this and said, "Our system is yet to be fully developed and so to be safe from sudden loss of all the information, we are keeping both paper and digital formats of our records".

Table 4.1 Beginning of digital preservation in the studied departments

Department	Year preservation of digital records commenced
M	1997
B	2000
D	2004
F	2004
G	2006
K	2010
L	2010
H	2011
E	2012
A	2012
C	2013
I	2013
J	2013

4.3.2 Records classes preserved in Masvingo

In all the departments, that is, A, B, C, D, E, F, G, H, I, J, K, L and M, officers interviewed concurred in their responses that their departments preserve financial and accounting, as well as administration records classes. The records management officer at Department L elaborated on these classes and said, "We keep financial and accounting records such as budgets, financial reports, proof of payments and audit reports as well as administration records such as correspondences, policy files, minutes of meetings, memoranda, asset registers, contracts and agreements". Participants in departments A, C, E, F, I, J, K, and M reported that they have records that can be classified as projects and programmes. In this class the IT officers in Departments F and I reported that they have records like circumcision programmes files, HIV and AIDS awareness and testing campaigns. The records management officer at Department M said, "In the projects and programmes class, we have records such as those to do with land development and construction of capital projects". At Department C the top administration officer said, "In the projects and programmes class we mainly have rural electrification projects files". The IT officers at Departments G and I reported that they also keep records classified as patients' records. The IT officer at Department I elaborated and said, "In the patients' records class, we mainly preserve in-patients' morbidity and mortality records". The top administration officer at Department B said, "On top of financial and accounting, and administration classes, we also keep records that are classified as human resources records such as staff performance appraisals and leave applications". In departments A, C, D, E, F, G, H, I, J, K, L and M, the researcher noted through interviews and observation that human resources records were stored in the manual system. The IT officer at Department H also said, "On top of financial and accounting, and administration classes, we also preserve records classified as student records in a database". The classes of records preserved in the case study departments are further illustrated in Table 4.2.

Table 4.2 Records classes preserved in the case study departments

Class of records	Department(s) preserving them
Financial and accounting	A, B, C, D, E, F, G, H, I, J, K, L and M.
Human resources	B
Administration	A, B, C, D, E, F, G, H, I, J, K, L and M.
Patients records	G, I
Students records	H
Projects / programmes	A, C, E, F, I, J, K, and M.

4.3.3 File types preserved by the studied departments in Masvingo

Participants in all departments studied (A, B, C, D, E, F, G, H, I, J, K, L and M.) reported during interview sessions that they preserve word processing documents, spreadsheets, presentations, electronic mail and web pages. The records management officer at Department M reinforced this and said, "Word processing documents, spreadsheets, presentations, electronic mail and web pages constitute the greater chunk of the digital records we preserve here". IT officers and records management officers in departments B, C, D, F, G, H, I, L and M confirmed that they keep databases. The IT officer at Department M elaborated and said, "We preserve databases of all our clients, stakeholders and debtors". Administration officers and IT officers in departments A, D, F, G, H, K, L, and M reported that they had started keeping records generated or received through social media platforms. The top administration officer at Department D remarked and said,

> Our department has embraced technology and we are now preserving information we instantly generate and share with our large clientele, through our Facebook page and Twitter handle. We are also preserving invaluable feedback we get from our clients which is adding value to our marketing strategies and growth of our industry and products.

The IT officer at Department F shedded more light on the records they preserved from social media platforms and said, "Most of the social media records we preserve are those that are generated or received through Facebook, followed by Twitter and to a limited extent videos that are shared through YouTube".

Records management officers in departments A, D, E, F, K, H and M confirmed during interviews that they preserve videos and images. The records manager at Department K justified preserving such records and said "As a heritage institution, videos and images are an integral part of our collections and they add meaning to what we explain verbally to both local and international consumers of our heritage products". Records management officers and top administration officers in departments A, D, F, K and M added that audio or sound files were also part of the records they preserved. The top administration officer at Department A emphasised and said, "We are preserving audio files which we use to relive certain functions we held in the past and the files are also evidence of who said what and how he or she expressed it". The file types preserved in the studied departments are further illustrated in Table 4.3.

Table 4.3: File types preserved in the studied departments

File types	**Department(s) preserving them**
Word processing documents	A, B, C, D, E, F, G, H, I, J, K, L and M.
Spreadsheets	A, B, C, D, E, F, G, H, I, J, K, L and M.
Audio	A, D, F, K and M
Video	A, D, E F, K, H and M
Images	A, C, D, F, H, K and M
Databases	B, C, D, F, G, H, I, L and M
Presentations	A, B, C, D, E, F, G, H, I, J, K, L and M.
Electronic mail (Email)	A, B, C, D, E, F, G, H, I, J, K, L and M.
Web pages	A, B, C, D, E, F, G, H, I, J, K, L and M.
Social media	A, D, F, G, H, K, L, M

4.3.4 Selection of digital records for preservation

The responsibility for selecting digital records for preservation in government departments in the province lies with the head or supervisor of the records management section. Records management officers in departments (H, I and M) concurred that they were guided by their retention and disposal policies to select digital records for preservation. The records

management officer at Department M remarked that, "We are guided by our retention and disposal policy to select records for preservation as you are aware that records management is a profession with instruments, policies and ethics that should be adhered to". However, in departments A, B, C, D, E, F, G, J, K and L, the researcher through interviews and observation noted that these departments were not adhering to the government position and heads of all sections within their departments were just using their discretion in selecting records for preservation. The scenario can be summarised by the response from the records management officer at Department L who said, "Heads of all sections within our organisation use their discretion on what to preserve and what to discard and in some instances everything is sent for preservation since there are no guiding principles". A top administration officer at Department F elaborated on this situation and said,

> We have delegated the task of selecting records for preservation to the heads of sections. We have entrusted them as experts in their areas with the task of selecting records worth preservation from their sections.

4.3.5 Preservation responsibility

This research established that departments C, F, H, I, J and M have bestowed preservation of digital records upon IT officers. The top administration officer at Department J confessed and said, "The issues of digital records preservation are problematic and too technical for some of us who never received training in that area and consequently we saw it fit to give the responsibility to the IT officer who is well versed with ICTs". However, the IT officer at Department H complained and said, "I am overloaded with the records management functions at the expense of my core duties like maintaining network, user support, configuring user accounts and hardware and software installations".

When the registry officers in the departments with IT officers were asked why they were not taking responsibility to preserve digital records, their answers can be summarised in the response from the records management officer at Department J who said, "I am not conversant with the management and preservation of digital records since I am used to the manual system which I am in charge of". In departments A, B, D, E, G, K, and L, the preservation function was bestowed upon the registry officers. A top administration officer at Department L's response summarised the sentiments of officers in these departments and had this to say,

"Records are records, whether on paper or in digital format and so a modern records manager must know how to manage and preserve them as he or she is an expert in that field".

4.3.6 Ingestion of digital records in Masvingo Province

As alluded to in Chapter One on conceptual framework, ingestion is a set of processes for accepting information submitted by producers and preparing it for inclusion in the archival store. Specific functions performed at this stage include receipt of records and validation that the records are uncorrupted and complete. Additionally, there is also transformation of the submitted records into a form suitable for storage and management within the archival system. Furthermore, ingestion includes extraction or creation of descriptive metadata and transfer of the records and their associated metadata to the archival store (DPC 2014:12). In all the studied departments, the researcher observed personnel charged with the preservation of digital records screening them for viruses and checking if they open before uploading them for preservation. Besides that, they were also making multiple copies of the records, which they store in different locations and on external storage media.

However, all the records management and IT officers who participated in this study showed a shallow understanding of the ingest process. In all the departments (A, B, C, D, E, F, G, H, I, J, K, L and M), interviews and document review yielded that there were no submission agreements between the records creating sections and those charged with their preservation as prescribed by the OAIS model. All the officers who participated in this study admitted that they were just preserving their digital records without guidelines and adherence to any standard(s). Responses from participants in departments (A, B, D, E, F, J and K), showed that heads of sections were just submitting their digital records for preservation in an *ad hoc* fashion. The IT officer at Department F lamented and said, "Since there are no guidelines for preparing digital records for archival storage or written down submission agreements, it is very difficult for heads of sections to transmit digital records for preservation in a systematic way or at pre-determined intervals". The departments also showed ignorance about packaging their records into Submission Information Packages (SIPs) in line with the OAIS model requirements. On the other hand those charged with the preservation function in departments A, B, D, E, F, J and K had their own challenges as elaborated by the IT officer at Department J who said,

We do not know how to appraise records that come to us haphazardly and we do not have an automated validation system to verify the integrity, completeness and correctness of the transferred records. There is no quality assurance or guidelines to verify authenticity and we just upload the records without attaching sufficient metadata.

4.3.7 Digital preservation strategies used in Masvingo Province

In line with the OAIS reference model, preservation strategies should be carefully selected and their implementation should be well planned. This is crucial in order to safeguard records from changes and risks due to new innovations in the storage and access technologies or a shift in the scope or expectations of the designated community. This research established through interviews and observation that the studied departments are using the following digital preservation strategies:

- Backup and byte replication.
- Migration.
- Printing and filing.
- Capturing preservation metadata.
- Cloud computing.

The usage of each strategy is further illustrated in Table 4.4.

Table 4.4: Digital preservation strategies used in the studied departments

Digital preservation strategy	**Department(s) using the strategy**
Backup and byte replication	A, B, C, D, E, F, G, H, I, J, K, L and M.
Migration	A, C, D, E, F, H, I, K, L and M.
Printing and filing	A, B, D, E, F, I, J, K and L
Capturing preservation metadata	C, F, G, H, I, L and M
Cloud computing	A, D, F, G and M

4.3.7.1 Backup and byte replication

Through interviews, this study established that backup and byte replication was used in all the thirteen departments studied. The IT officer at Department F said, "We make multiple copies of files and store them in different locations and external storage media". There was also a general view from all the IT and records management officers that the strategy was easy to implement. This was reinforced by the records management officer at Department K who said, "The strategy's major attraction is that it requires little technical expertise yet it can serve records from hardware and software failure, intentional or unintentional alterations as well as disasters". The researcher also observed the IT officer at Department F saving programme files into a computer folder and on both external hard drive and USB flash drive for backup purposes.

4.3.7.2 Migration

Migration was used in departments (A, C, D, E, F, H, I, K, L and M). This was further qualified by the IT officer at Department D who said, "We largely migrate our records from one file format to another and also from one version of system to another". The file formats departments were migrating their files to, are shown in Table 4.5. Both the IT and records management officers in departments using this strategy concurred that the method was giving them problems. The IT officer at Department F remarked that, "We lost some of our information in 2014 when we migrated from the old system to a new system we are using now and at the moment we are using the strategy to convert some of our files to stable formats". The records management officer at Department L bemoaned and said, "One thing I hate about migration is that it is time consuming and often changes the structure of information to the extent that you will have to start the whole process over again".

Through interviews and observation, this research also established that none of the departments was practising migration by normalisation whereby the data file is converted to an open format such as Open Document Text (.odt) for word processing documents, Open Document Spreadsheets (.ods) for spreadsheets, SIARD for databases and Open Media Framework for videos, and Open Document Presentation (.odp) for PowerPoint presentations.

Table 4.5: File formats used in the studied departments

File format	Departments using the format
Portable Document Format (PDF)	A, B, C, D, E, F, G, H, I, J, K, L and M
Rich Text Format (RTF)	A, C, and E
Microsoft Word Document (DOC)	A, C, D, E, G, H, J, K and M
PDF/A-1a / (ISO 19005-1: 2005 compliant PDF/A)	-
XML (.xml) with DTD/Schema	-
Standard Generalised Markup Language (SGML), with Document Type Declaration (DTD) /Schema	-
Microsoft Excel Spreadsheet (XLS)	D, and H
Open Document Spreadsheet (ISO/IED 26300:2006) (ODS)	-
Comma-separated file (.CSV)	-
Moving Picture Experts Group (MPEG-3) (mp3)	A, D, F, K and M
Broadcast Wave Format encoded with Linear Pulse Code Modulated (LPCM) (.wav)	-
Moving Picture Experts Group MPEG 4 (mp3)	A, D, E, F, K, H and M
Open Media Framework (OMF)	-
Joint Photographic Experts Group (JPEG)	A, C, D, F, H, K and M
Joint Photographic Experts Group (JPEG 2000/ ISO 15444-1p:2004)	-
Database format (.dbf)	B, C, D, F, G, H, I, L and M
Software Independent Archiving of Rational Databases (SIARD)	-
Microsoft PowerPoint Presentation (.ppt)	A, B, C, D, E, F, G, H, I, J, K, L and M
Open Document Presentation (ISO/IED 26300:2006) (.odp)	-
Microsoft Outlook Personal Storage Table (.pst)	-
Web Archive (ISO 28500:2009) (.warc, or .war)	-

4.3.7.3 Printing and filing

Through interviews and observation, this research established that departments (A, B, D, E, F, I, J, K and L) were printing into hard copies and filing into their manual system some of their digital records usually those transmitted through electronic mails (e-mails) and on their websites and social media platforms. The records management officer at Department G expounded and said,

> Our system is not fully developed and we do not have adequate trust on the digital system. As a result, we print and file in order to be safe from loosing valuable information especially e-mails. However, it is proving difficult to preserve all the e-mails since most officers are using their personal commercial accounts like Gmail and Yahoo for official business. We are also stuck on ways of harvesting and preserving information on our website and social media platforms electronically and hence we again print and file it. We did not receive adequate training on how most of the digital preservation strategies work as we just learnt about them in passing without any practical demonstration on how they can be implemented.

The administration officer at Department A echoed similar sentiments and said, "Printing and filing is easy even for some of us who do not have sophisticated skills in ICTs and records management".

4.3.7.4 Capturing preservation metadata

Through interviews, this research also established that departments (C, F, G, H, I, L and M) were capturing preservation metadata as a preservation strategy. The researcher was getting responses from these departments which can be summarised in the words of the records management officer at Department H, who said,

> We are capturing metadata of the records we preserve as a way of guaranteeing their easy and continued access in the future. Although we are not conforming to any set of standards, we highly value capturing metadata in our preservation efforts because it makes it faster to identify and retrieve the needed information embedded within huge volumes of records. Capturing adequate metadata is also invaluable for maintaining the integrity and authenticity of our records.

On the contrary, departments A, B, D, E, J and K were ignorant about both metadata standards and the value of capturing metadata in their digital preservation efforts. The records management officer at Department J lamented and said,

> We do not have much enlightenment on metadata and hence we are not capturing it. However, although we do not possess adequate knowledge and skills for preserving digital records, NAZ as the institution mandated to store and preserve all records is also to blame because it has not only left the role to us the creating departments, but is neither giving us adequate guidance in the management and preservation of digital records as they do with paper records through records management surveys nor prescribing preservation systems and softwares that conform to archival standards.

4.3.7.5 Cloud computing

Cloud computing or storage strategy was used in departments (A, D, F, G and M) for preserving some of their records. However through document analysis, this study established that there was no policy or guidelines authorising the use of cloud storage. The general reasons departments cited for using cloud computing can be summarised in the response of the administration officer at department D who said, "We opted for cloud storage because it saves us money due to reduced pressure to provide increasing storage capacity". The IT officer at Department M also remarked that, "Cloud computing lessens server maintenance tasks". On the other hand, departments B, C, E, H, I, J, K and L were not storing their records in the cloud. The top administration officer at Department H explained and said, "We are not storing our records in the cloud for security reasons since most of our records are very confidential". The records management officer at Department L concurred and said, "Our records are so sensitive that we could not risk the integrity of our organisation through entrusting a third part to preserve them on our behalf, and that is why our institution sacrificed to purchase a server for us to store the records at our institution with backup at our national office in Harare.

4.4 Legal, standards and policy guidelines

The second objective of this study was to analyse legal, standards and policy guidelines supporting the preservation of digital records. In line with the OAIS reference model, there is need to have clear policies and procedures for carrying out the preservation of digital records.

Furthermore, the policies and procedures must be understandable by all the stakeholders and include a clear plan that covers the disposition of these records (DPC 2014). As already highlighted in the literature review in Chapter Two, adhering to legal, standards and policy guidelines is an anchor to effective preservation of digital records. Legislation has a tremendous impact on how records including those that are created and stored in networked environments are managed in any country (Ngoepe and Saurombe 2016). The use of standards and policy guidelines has long been a cornerstone of the information industry since they facilitate access, discovery and sharing of digital resources as well as their long term preservation (DPC 2016b). The research findings on these issues are further elaborated in subsections 4.41 to 4.4.3.

4.4.1 Legal framework

The legal framework for management and preservation of records in Zimbabwe is the NAZ Act Chapter 25:06 of 1986. However, through interviews, this study discovered that departments (B, C, D, and F) had no knowledge about the NAZ Act. The IT officer at Department F confessed and said, "I have never heard about the NAZ Act and as a department, we have never transferred even our paper records to the NAZ Provincial Records Centre". The other departments that is, A, E, G, H, I, J, K, L and M had knowledge about the Act but they largely scoffed at its shortcomings. The records management officer at Department M said,

> We are very unfortunate in the sense that the current National Archives Act has little meaning when it comes to the management and preservation of digital records. No one listens to our concerns when we want to advance digital preservation issues due to lack of a strong reference point in the Act in terms of clear instructions on creation, storage, appraisal, destruction and preservation of digital records.

The records management officer at Department E echoed similar sentiments and said,

> Our digital preservation strategies are weak as the legal framework is also weak. We are failing to operate with authority as the Act neither gives us the mandate to preserve digital records nor spells out detailed practices and procedures for preservation of these records.

4.4.2 Digital preservation standards

Through interviews, this study established that all the participants in the studied departments were not aware of digital preservation standards like the OAIS model (ISO 14721:2003); ISO/TR 18492:2005- Long Term Preservation of Electronic Document based Information; ISO/IEC 27001:2013 - Information Technology - Security Techniques - Information Security Management Systems - Requirements and metadata standards or schemas such as PREMIS; METS; Dublin Core and EAD. Responses from most of the participants and especially the records management officer at Department J affirmed this as she said, "At this department, we have no knowledge about any digital preservation standard and we are also now hearing that there are what are called trusted digital repositories for preserving digital records which we neither have nor have seen".

Participants in departments A, B, C, D, E, F, G, I, J, K, L and M failed to give answers to the question, "Which standard(s) does your organisation benchmark against its digital preservation?" Only department H had a preservation system that was compliant to the Standards Association of Zimbabwe (SAZ) ISO 9001:2008- Quality Management Systems: Requirements. However the standard is just general and does not address specific requirements for records management and preservation. The IT officer at Department H lamented and said, "We just adopted our system without consulting the National Archives for informed guidance but the system so far is doing us a good job". The records management officer at Department H also said, "We bench-mark our preservation efforts to the institution's regional procedures manual". However, through document analysis, this study established that the manual had much on the management and preservation of paper records than the digital records since it lacked clear instructions about selecting and ingesting digital records into the preservation system.

4.4.3 Digital preservation policies and guidelines

This research through interviews and document analysis established that departments A, B, D, E, G, I, J and K lacked written crucial documents to support their preservation work. The records management officer at Department K's response summarised the responses of the participants in these departments. He said, "We lacked written documents like preservation policy, access policy, security and privacy policy and guidelines for handling storage media, as

well as social media policy or guidelines". Responding to the probing up question why they had no policies, the general response from departments such as B, D, E, J can be summarised in the words of the records management officer at Department J who said,

> The issue of policies looks like both a national and departmental problem because on one hand we are lacking a national framework governing the management and preservation of digital records and on the other hand as records management practitioners we are now reluctant since we are fed up of having policy documents without the necessary resources to execute tasks stipulated in the policies.

Through document analysis, this study established that departments C, F, and M had ICT policies. However through thorough analysis of the documents, this research also established that these policies had more to do with how ICT gadgets should be used and maintained as well as procurement procedures for hardware and software packages and connectivity issues. The policies were silent about digital records management and preservation issues. The general response from administration and IT officers in departments that do not have ICT policies at all, can be summarised in the response of the records management officer at Department J who said, "We are waiting for the national ICT policy document being worked on by the Ministry of Information, Communication Technology and Courier Services so that we can as well start working on our departmental guidelines".

Document analysis also yielded that departments H, L and M had retention and disposal policies. However through thorough review of the documents, this research established that the policies were much applicable to paper records as they lacked specific instructions on how to dispose digital records and by whom. Retention and disposal policies were absent in departments A, B, C, D, E, F, G, I, J and K, and this research discovered that retention and disposal was not properly done. This was reinforced by the response from the top administration officer at Department F who said, "Retention and disposal of digital records is done at the discretion of the officers charged with the preservation of the digital records and there are no guidelines or expertise to carry out appraisal of these records". The IT officer at Department K said, "I am not aware of an instrument called retention and disposal policy for it is not common in IT vocabulary".

4.5 Infrastructure, resources and tools for digital preservation

The third objective of this study was to access infrastructure and resources to carter for the preservation of digital records. This study established through interviews and observation that all the departments studied had client computers in the form of either desktops or laptops or both. The IT officer at Department F reiterated and said,

> Our systems are not fully developed and hence our preservation efforts start here on the client computer where some records are stored in electronic folders and on the computer hard drive. The client computers are connected to a server through a network.

The records management officer at Department B reported that their server size is 500 gigabytes. The administration officers in departments A, E and J reported that they have one terabyte (1TB) servers. Records management officers in Departments C, D, F, G, H, I, K and L said that they have 1.5Terabytes (TB) servers. The IT officer at Department M reported that they have a six terabyte (6TB) server. Participants in all the studied departments reported that they have external hard drives mainly for backing up their digital records. Records management officers in departments A, D, F, G and M reported that they are using cloud storage to preserve some of their records. Participants in all the studied departments said that they have internet connection. However, there were general complains that can be summarised in the words of the IT officer at Department M who said, “Our internet is very slow and weak especially when uploading large volumes of records”. Participants in all the studied departments said that they have Local Area Network (LAN). Records management officers in departments D, F, H, L and M reported that they have both LAN and Wide Area Network (WAN). The preservation infrastructure in the studied departments is further illustrated in Table 4.6.

However, the general remarks by all the participants were that the infrastructure and resources for preservation of digital records were inadequate and the systems were not fully developed to allow for interoperability in the event of a change in the hardware and software environment. One top administration officer at Department M commented and said,

> As a department we cannot be solely blamed for this situation because according to the law of the country, the role of preserving all records including these digital ones is the mandate of the National Archives of Zimbabwe. They are the ones

> who should be having well developed systems and infrastructure to absorb for preservation those records of enduring value our systems are generating. The infrastructure that we have can be best described as makeshift just to avoid the loss of valuable information and we feel betrayed by the national archival institution.

Through interviews and observation, the researcher also noted the use of CDs in departments A, E, H, K and M; Digital Versatile Disks (DVDs) in departments A, H, K and M, computer tapes in Department M and USB flash drives in departments A, D, E, F, G, H, I, J, K and L for backing up their records. Records management officers in departments C, G, H, I, L and M reported that they have generators for power back up. Administration officers in departments A, B, D, E, F, I, J, K and L informed the researcher that they have no specific budgets for preservation of their digital records. Responding to a follow up question why there was no budget, the records management officer at Department I said, "As records and information management section, we are so much looked down upon by top management to the extent that our concerns are always not a priority". In departments C, G, H, and M that reported of having budgets, the administration, records management and IT officers concurred that the budgets they were getting to carry out digital preservation were erratic and inadequate. Table 4.6 gives a summary of infrastructure and resources for preservation of digital records in the studied departments in Masvingo province.

Table 4.6: Infrastructure and resources for digital preservation

Equipment/ resource/ facility	**Departments having the equipment/ resource/ facility**
Client computers	A, B, C, D, E, F, G, H, I, J, K, L and M.
servers	A, B, C, D, E, F, G, H, I, J, K, L and M.
External Hard drives	A, B, C, D, E, F, G, H, I, J, K, L and M.
Cloud	A, D, F, G and M
Internet connection	A, B, C, D, E, F, G, H, I, J, K, L and M.
LAN	A, B, C, D, E, F, G, H, I, J, K, L and M
WAN	D, F, H, L and M
CDs	A, E, H, K and M
Blu-ray discs	-

DVDs	A, H, K and M
Computer tapes	M
USB flash drives	A, D, E, F, G, H, I, J, K and L
Secure Digital (SD) cards	-
Solid State Drives (SSD)	-
Power backup	C, G, H, I, L and M
Budget	C, G, H, and M
Cold room	-

4.6 Professional knowledge and skills levels of staff

Information is a valuable asset and like other assets such as vehicles, buildings or money, its management requires professionals with appropriate capabilities, skills and knowledge (National Archives of Australia 2017). In accordance with the OAIS reference model, a person responsible for preserving digital records should know how to assign AIPs to permanent storage according to various criteria like media requirements and expected utilisation rates. In addition to that, he or she must be able to migrate AIPs to new media as required, check for error, implement disaster recovery strategies and provide copies of requested AIPs to the access function. Through interviews, this research established that the top administration officers had qualifications illustrated in Table 4.7. However, all these qualifications were not inclined to records and archival management or information science.

Table 4.7: Educational background of administration officers

Department	Job title	Educational Qualification	Area of Specialisation
A	Provincial head	Masters Degree	Media
B	Provincial head	First Degree	Environmental Science
C	Provincial head	Masters Degree	Electrical Engineering
D	Provincial head	First Degree	Tourism and Hospitality
E	Administration officer	First Degree	Agriculture
F	Administration officer	Diploma	Office Administration
G	Accountant	First Degree	Accounts
H	Accountant	Higher National Diploma	Accounts
I	Human Resources Officer	First degree	Human Resources
J	Administration officer	Diploma	Purchasing and Supply
K	Administration officer	Masters Degree	Archaeology
L	Human Resources Officer	First degree	Human Resources
M	Human Resources Officer	First Degree	Human Resources

Through interviews, this study established that the records management officers in the studied departments had qualifications in records management and information science at levels illustrated in Table 4.8. The content of these qualifications were not investigated. However, despite having the relevant qualification for their job, most of them were still lamenting that they lacked the practical know-how and skills to execute most of their digital records preservation duties. The records management officer at Department J said,

> Our department have not been prioritising staff development in the past five years due to economic hardships and partly because we are headed by officers who place little importance on records management issues. The National Archives used to carry-out training workshops for us on paper records management issues but since we started having some of our records in digital format, they are nowhere to be seen. We lack basic skills in appraisal, management and preservation of digital records.

Table 4.8: Qualifications of records management officers

Department	Records management officers' qualification(s)
A	Diploma in Records Management and Information Science
B	Certificate in Records Management and Information Science
C	Diploma in Records Management and Information Science
D	Certificate in Records Management and Information Science
E	Certificate in Records Management and Information Science
F	Diploma in Records Management and Information Science
G	Diploma in Records Management and Information Science
H	Bachelor of Science Degree in Records and Archival Management
I	Diploma in Records Management and Information Science
J	Diploma in Records Management and Information Science
K	Diploma in Records Management and Information Science
L	Bachelor of Science Degree in Records and Archival Management
M	Diploma in Records Management and Information Science

Through interviews, this research also established the qualifications of the IT officers as illustrated in Table 4.9. The general comment from these officers can be summarised in the utterances of the IT officer at Department J who said,

> I am lagging far behind the pace of technological developments as a professional due to lack of budgets for purchasing modern machines and softwares, as well as for continuous training. This is greatly compromising my efficiency in executing my duties. The department has been failing to send me for workshops, conferences or seminars since 2013.

Table 4.9: Educational levels of the IT officers

Department	IT officers' qualification(s)
C	Degree in Information Systems
F	Degree in Information Technology
H	Degree in Information Technology
I	Diploma in Information Science Technology
J	Diploma in Information Science Technology
M	Diploma in Information Science Technology

4.7 Access, security and privacy issues

It is critical to ensure that security and access measures are in place when preserving digital records as authentic evidence for the long term in order to protect records from unauthorised change or deletion (IRMT 2009:25). In line with the fifth objective of this study as outlined in Chapter One, this section sought to provide answers to the following questions,

- Who have access to the preserved digital records?
- How is access and security to the preserved digital records provided?
- What security and privacy challenges do institutions encounter?
- How do departments protect their digital records from unauthorised access?
- How do departments protect their digital records from tempering?
- How do departments protect their digital records from viruses?
- What plans are in place to salvage digital records in the event disaster strikes?

4.7.1 Accessibility of the preserved digital records

In relation to access to the preserved digital records, the OAIS reference model stipulates that contents of the archival store should be made available to the intended user community through the implementation of access mechanisms and services which support user needs and requirements. Furthermore, access restrictions attached to some or all of the archive's contents should be clearly documented. The general response to the question on accessibility of the preserved digital records can be summarised in the word of the records management officer at Department G who indicated that,

> All employees at officer grade and above have access to the preserved digital records. However, general hands and security guards are excluded from the privilege of having access to the preserved digital records.

All the participants reiterated that their departments have defined levels of access or access rights that are in line with the duties of each officer. Both records management and IT officers reported that heads of sections in their departments had more access rights slightly lower than that of provincial heads who have access to all the records. The provincial head at Department C said, "I have access to all the records as I am at the helm of everything at provincial level".

4.7.2 Provision of access to the preserved digital records

The general response to this question across the studied departments can be summarised in the words of the IT officer at Department M who said, "Access to the preserved records is online from server storage through user authorisation and authentication processes". However administration officers in departments A, B, D, E, F, J and K complained that accessing some of the digital records was a mammoth task due to poor arrangement, description and indexing. Moreover, they also reported that some records were preserved without accompanying metadata. Through document analysis, this study established that all the departments were operating without a written access policy. Interviews with records management and IT officers revealed that they were ignorant about the Access to Information and Protection of Privacy Act Chapter 10:27 (AIPPA) that regulates the provision of access to information in Zimbabwe.

4.7.3 Security and privacy relating to digital records

This study through interviews established the following security and privacy challenges in the studied departments:

- Hacking of files by outsiders.
- Viruses.
- Crushing of machines.
- Deletion of files.
- Unauthorised access.
- Files left open on shared client computers.
- Migration errors.

- Technological obsolescence.

Participants in departments C, F and J reported that they were experiencing the challenge of files left open on shared client computers and unauthorised access. The records management officer at Department C remarked that, "Our greatest challenge so far is that users at times leave copies of the digital records they would have accessed open on user devises that are shared in the department giving chance to unauthorised access". Administration officers in departments F and K reported that they were grappling to contain the threat of viruses and crushing of machines. Hacking challenge was also reported by the records management officer at Department L who said, "We have an incident about two years ago whereby outside identity thieves hacked and stole some documents from our system".

Deletion of records was also cited as a disturbing challenge by participants in departments B, E, F, J, K and L. Elaborating on the challenge of losing information during migration as also reported by participants in departments E, I and M, the IT officer at Department F said, "We lost some of our information in 2014 when we migrated from the old system to a new system we are using now". The IT officer at Department M echoed similar sentiments and said, "We permanently lost some of our records when we tried to transfer records that were not backed-up to the upgraded system when the session failed". The IT officer at Department M also reported that they were having technological obsolescence challenges. He said, "Some of our digital records on computer tapes are now failing to read due to sticking and breaking of the magnetic ribbon". These challenges are further illustrated in Table 4.10.

Table 4.10 Security and privacy of digital records

Security and privacy challenge	**Departments affected**
Files left open on shared client computers	C, F and J
Unauthorised access	C, F and J
Viruses	F and K
Crushing of machines	F and K
Hacking	L
Deletion of records	B, E, F, J, K and L
Migration errors	E, I, F and M
Technological obsolescence	M

4.7.4 Protection of digital records from unauthorised access and tempering

Participants in the case study departments reported that they protect their preserved records from unauthorised access through user authorisation and authentication processes. Elaborating further, the IT officer at Department F said, "Authentication and authorisation are ways to intelligently control access to computer resources and auditing usage". Through further probing she explained that, "authentication provides a way of identifying a user by making the user to enter valid username and password before access is granted, and the authorisation process defines the types or qualities of activities, resources or services the user is permitted by the system". All participants reported that authentication and authorisation were also used as protection of the records from tempering. Besides authentication and authorisation, registry officers in departments A, I and L added that they use encryption to further safeguard their records from unauthorised access and tempering. Interviews with all the administration officers in the studied departments also established that they used lock and key on records storage rooms to control unauthorised access. In departments B, C, F, G, H, L and M, the administration officers highlighted that they have security guards manning entrances to their premises to further monitor unauthorised access. Table 4.11 further illustrates how departments protect their records from unauthorised access and tempering.

Table 4.11 Protection of digital records from unauthorised access and tempering

Protection method	**Departments using the method**
Authentication and authorisation	A, B, C, D, E, F, G, H, I, J, K, L and M
Encryption	A, I and L
Electronic signatures	-
Lock and key	A, B, C, D, E, F, G, H, I, J, K, L and M
Security guards	B, C, F, G, H, L and M
CCTV	-
Alarm system	-

4.7.5 Protection of digital records from viruses and malicious software

Through interviews, this study established that all departments were using antivirus software to protect records from viruses. Participants in all the studied departments reported that they also use the backup strategy again as a measure to reduce the adverse effects of viruses. IT officers in departments F, H and J added that they also used firewall against viruses and malicious software. However the IT officer at Department K lamented and said, "Our department is relying on free antivirus software from the internet which at times is outwitted by stronger malicious software and the challenge led to the crashing of some of our machines in 2013". The protection mechanisms used in the studied departments are further illustrated in Table 4.12.

Table 4.12 Protection of records from viruses and malicious software

Protection method	**Departments using the method**
Antivirus	A, B, C, D, E, F, G, H, I, J, K, L and M
firewall	F, H and J
Back up	A, B, C, D, E, F, G, H, I, J, K, L and M

4.7.6 Protection of digital records against disasters

Through interviews, the participants in the studied departments gave the following as potential causes of disasters in their departments:

- Uncontrolled humidity.
- Uncontrolled temperature.
- Sunlight.
- Water.
- Fire.
- Dust.
- Pests.

Through document analysis, this study yielded that departments H and M had written disaster management plans. However the disaster management plans had much on salvaging paper

records than the digital ones. The disaster plans were silent about tackling threats and vulnerabilities of digital records such as migration errors, software obsolescence, disk crushes and bit rot. In his response, the IT officer at Department M acknowledged these weaknesses and said, "I think our disaster management plan now needs to be reviewed as it does not address potential risks to our digital records". Interviews and document analysis also revealed that departments A, B, C, D, E, F, G, I, J, K and L had no written down disaster management plans. The IT officer at Department F said, "We do not have a written disaster management plan but we rely on the backup strategy and storing our digital storage media in different locations as a measure to mitigate the effects of potential disasters". The top administration officer at Department D also said, "We rely on cloud storage for safety of our records against disasters.

Through observation and interviews, this research also established that all the surveyed departments had control measures against natural radiation, water and magnetic fields. However, records management officers in departments F, I and J reported that their digital records were not safe from pests. The records management officer at Department I lamented and said, "Our kitchen is too close to the records storage area and most employees are also taking their food close by leaving a lot of food debris that have attracted cockroaches and rodents in our premises". Participants in departments A, B, C, D, E, G, H, K, L and M reported that they are using fumigation to control pests.

Although there were fire extinguishers in all the surveyed departments, this research established through interviews and observation that departments C, D, F, G, H, K, L and M were better prepared in the event of fire outbreak. These departments had also horse reels to augment the fire extinguishers. Departments C, D and L had smoke detectors in their premises and records storage areas. Departments A, B, E, I and J had extinguishers that were due for service. The records management officer at department I confessed and said,

> Our fire extinguishers were installed long ago and are not regularly serviced. As we speak right now they have already passed their service due date. Staff members were not trained on how to use them and mock fire fighting drills have never been conducted.

The records management officer at Department J also said,

> I think the failure to service fire fighting equipment is due to negligence by top management officers who always look down upon the records management section and not necessarily limited finances. Our section is always at the bottom of the priority list in terms of allocation of resources.

Participants in all the studied departments reported that they have no means of controlling humidity, temperature and dust in their records storage areas. Table 4.13 further gives a summary of preparedness of departments to disasters.

Table 4.13: Preparedness of departments to disasters

Disaster preparedness measure	**Departments using the measure**
Disaster management plan	H and M
Backup	A, B, C, D, E, F, G, H, I, J, K, L and M
Cloud Storage	A, D, F, G and M
Thick curtains to prevent sunlight	A, B, C, D, E, F, G, H, I, J, K, L and M
Fumigation	A, B, C, D, E, G, H, K, L and M
Serviced fire extinguishers	C, D, F, G, H, K, L and M
Air conditioning system	-
Smoke detectors	C, D and L
Fire horse reels	C, D, F, G, H, K, L and M
Dehumidifiers	-
hygrometers	-
Dust filters	-

4.8 Summary

This chapter presented data gathered through interviews, observation and document analysis from 13 departments to address the research questions presented in Chapter One in line with the objectives of the study. It emerged that the surveyed departments in Masvingo started to preserve digital records at different intervals stretching from 1997 to 2013. However, the departments showed that they still have challenges in selecting records for preservation and properly ingesting them. The preservation systems were also not well developed and did not

conform to standards such as the OAIS reference model. The digital preservation initiatives in the studied departments were faced with challenges such as lack of adequate resources and budgets, suitable infrastructure, skilled personnel, legal, policy and standard(s) guidelines. The next chapter covers the interpretation and discussion of the findings of this study. In addition to that, the chapter also compares the findings with those from other related empirical studies where a similar phenomenon was investigated.

CHAPTER FIVE
INTERPRETATION AND DISCUSSION OF FINDINGS

5.1 Introduction

This chapter discusses and interprets the data presented in chapter four of this study. The chapter is important because it is usually considered the heart of the research by providing answers to the research questions. Furthermore, it explains how the results support the answers and how the answers fit in with existing knowledge on the topic (San Francisco Edit 2017). This chapter is also invaluable as it states interpretations and opinions, and explains the implication of the research findings (San Francisco Edit 2017). Additionally, it explains the meaning of the research results to the reader (Hess 2004:1239). The interpretation and discussion was done with the research problem, research questions, literature review and conceptual framework in mind. The findings were also compared with those from other related studies especially in the ESARBICA region and sub-Saharan Africa where a similar phenomenon was investigated. The sections of this chapter were arranged in line with the first five research questions of this study outlined in Chapter One as follows:

1. What strategies are used to preserve digital records to ensure their continued accessibility?
2. What legal, standards or policy guidelines are in place to support the preservation of digital records?
3. What infrastructure and resources are available to cater for the preservation of digital records?
4. What levels of professional knowledge and skills do staff responsible for preserving digital records possess?
5. How is access and security to the preserved digital records provided?

5.2 Strategies for preservation of digital records

Digital records preserved in Masvingo like policy files, contracts and agreements, programme and project files, patients' records, students' records as revealed in Chapter Four are of enduring value and require long-term preservation. File types preserved in Masvingo like e-mails, spreadsheets and databases containing patients, students and financial records useful to departments and individuals can pose a threat if proper security protections are not put in place

as shown in the literature review (Chapter Two). This means that the strategies for preservation of these records must be sustainable or applicable indefinitely into the future and appropriate or relevant to the types of records and metadata to be preserved (ICA 2016:46).

The findings of this research show that backup and byte replication, migration, printing and filing, capturing preservation metadata and cloud computing were the preservation strategies used in Masvingo province. The major reason participants cited for using these strategies was that they were cheaper for them as they were operating in a difficult economic environment where infrastructure, resources and budgets were hardly sufficient. Another reason raised by participants was that their records management sections were not prioritised in terms of resource allocation. The records management officers also conceded that they have limited technical skills and knowledge of how other strategies like emulation and encapsulation can be implemented. This situation greatly suggests that the strategies for preservation of digital records in Masvingo province are at the moment makeshift and interim in nature. The essence of preservation seems to have been poorly conceived and adopted without a preceding cost benefit analysis or digital readiness assessment.

Despite a fairly longer period of preserving digital records by some departments like M, B, D, F and G as shown in Table 4.1 of Chapter Four, the development of preservation strategies, skills and infrastructure has remained inadequate. The selection of digital records for preservation was being done by heads of sections who did not have records and archival management qualifications as shown in Table 4.7 of Chapter Four using their discretion. This leaves great room for destruction of records of enduring value and preservation of those of ephemeral value or just clogging the storage facility with records of questionable value that can only create difficulties in accessing required information (National Archives of UK:2011).

The strategies the province is currently using are compromising the long-term preservation of digital records. As illustrated in the literature review, Corrado and Moulaison (2014:4) argue that backup and byte replication alone cannot guarantee the perpetuity and longevity of digital records, because it provides short-term to medium-term strategy to extend the life of these resources.

On another angle, Ngoepe (2017) argues that cloud storage can only be considered as an interim option for preserving digital records because there are more issues around it that are against the norms of the records and archival management profession. Similar to the situation observed in South Africa by Ngoepe (2017), few departments in Masvingo have embraced cloud storage due to lack of policies and guidelines. Katuu and Ngoepe (2015) and also Branco and Santos (2015:4) expound that cloud storage has no guarantee of continued availability of stored data in an authentic and reliable form since data is put on computers you do not have control over. It is therefore crucial for departments solely relying on backup and byte replication and cloud storage to remodel their strategies for sustainability.

This study as illustrated in Table 4.4 established that the departments were yet to embrace open standard and non-proprietary formats in their migration efforts. This makes the records to be vulnerable to technological obsolescence challenges. Open formats allow for unlimited use without licence fees or patent issues and their fully available documentation eases their future handling (Barve 2007). Most of the departments were using proprietary formats such as Microsoft Word Document (DOC), Database format (.dbf), Microsoft PowerPoint Presentation (.ppt) and Moving Picture Experts Group MPEG 4 (mp3) that are not suitable for long-term preservation. TAHO (2015) argues that it is more advantageous for government entities to prioritise the use of non-proprietary and open standard formats that are more fully documented and more likely to be supported by tools for validation than proprietary formats. Furthermore, accepting all formats and committing to preserve them is unlikely to be successful (TAHO 2015).

This research also discovered that some departments were not capturing preservation metadata due to ignorance about its importance. This is a grave omission with far reaching negative consequences. As highlighted in the literature review (Chapter Two), metadata is crucial for the purposes of identifying, retrieving, managing and preserving digital records (InterPARES 3 Project: Team Canada 2013). Sugimoto (2014) adds that preserving both metadata and digital resources is crucial since loss or extinction of the metadata can render the records inaccessible and defeats the purpose of preservation. This scenario where some departments were ignorant about simple basics of preservation such as capturing metadata is testimony that preservation of digital records in Masvingo province is still at its infancy stages and much has to be done in practical training of those charged with the preservation of these records.

This study also found that the departments were printing and filing some of their digital records especially those transmitted through e-mails, social media platforms and website pages. Although this strategy seems easy to those with limited practical digital preservation techniques, it cannot be totally relied upon. Wright (2014) argues that some digitally created records do not translate well into a printed format for example, a print-out does not allow a user to click on links and audio and video files do not translate at all in a print-out. In other words, printing digital records also makes them no longer truly machine readable which in turn destroys their core digital attributes such as perfect copying, access and distribution among other things. This strategy in a way shows that digital readiness assessment was not thoroughly done and digital records were just adopted in Masvingo province when some basics such as skills and resources were still inadequate.

Through interviews and observation of the preservation systems used, this research established that all the thirteen departments were yet to use trusted digital repositories (TDRs), which can manage digital resources to their designated community now and in the future and are OAIS compliant. As was highlighted in the literature review in Chapter Two, identifying, collecting and storing online publications and organisational records will be a futile exercise if strategies such as developing TDRs are not devised (Ngulube 2012:114). A TDR offers security and can be audited to ensure appropriate performance and quality management (Adu 2015:81). The departments also lacked knowledge about preservation softwares such as Achivematica and Access to Memory (AtoM) that are compliant to archival standards like the OAIS model (ISO 14721:2003).

In light of the findings of this study, it is clear that the strategies for preservation of digital records currently used in Masvingo province do not guarantee their long-term preservation. As shown in Chapter Four of this study, NAZ also shares this blame. Some participants like the records management officer at department J were quick to point out that NAZ mandated to store and preserve all records had not only left the role to them but was not giving them adequate guidance in the management and preservation of digital records as they do with paper records through records management surveys (see Appendix vi). The findings of this research correspond well with Ngoepe (2017) who in his study entitled "Archival orthodoxy of post-custodial realities for digital records in South Africa" finds out that storage of digital records in creating agencies cannot be considered preservation for the future since many of these

institutions do not have the capability to locate and retrieve records after a certain period of time.

The findings also confirm Ngulube (2012)'s study on preservation of digital records in sub-Saharan Africa which established that there is still much ignorance about online tools and methodologies in the public sector for digital preservation in the region. Similarly, this study established that all the studied departments had no trusted digital repositories and were ignorant about preservation assessment toolkits like TRAC, NESTOR and DRAMBORA among others that are invaluable for certification process and risk assessment as well as software tools like DSPACE, FEDORA, LOCKSS and DAITSS among others crucial for generation of technical metadata to support the preservation of digital records. Digital records in Masvingo are therefore in danger of becoming irretrievable. Clear and consistent processes to monitor the integrity of the content, context and structure of all digital objects along with their metadata and to search for corruption or other alterations of the data as well as monitoring changes in technology, are critical to maintain high quality preservation strategies and to avoid costly data recovery activities (IRMT 2009).

The findings of this research also corroborates Ngulube (2012:115) who also notes that not much has been done to deal with concerns related to facilitating the capture and preservation of long term access to government records and publications in an ICT driven environment. Digital records in Masvingo are therefore at great risk of getting lost and this confirms the observations of Ngulube and Tafor (2006) who argue that access to public records and archives in the ESARBICA region is likely to diminish rapidly due to inadequate strategies and a dearth of knowledge of archival preservation techniques.

5.3 Legal, standards and policy guidelines

The National Archives Act is the legal framework for the management and preservation of all public sector records in Zimbabwe. However, participants in this study revealed that they were not getting much help from the provisions of the Act in terms of managing and preserving their digital records. Departments B, C, D, and F were also ignorant about the existence of the Act. As highlighted in Chapter Four, all the departments were not conforming to any digital preservation standard in their preservation efforts. The departments were also lacking crucial

documents like preservation policy, security and access policy and guidelines for handling storage media.

As was highlighted in the literature review, this situation of lack of or paucity of standards, policies and guidelines militates against effective digital preservation. It is the notion of this study, just as Wamukoya and Lowry (2013) would argue that digital records must be stored in trusted digital repositories in accordance with international standards, good practice and much documentation for their continued accessibility in the face of changing technology. The digital preservation scenario in Masvingo province appears much to be at its infancy stage and preservation activities are being carried out in an *ad-hoc* fashion due to lack of policy guidelines and standards.

The legal framework used (NAZ Act) has been criticised by most of the participants in this study as shown in Chapter Four. Furthermore, scholars like Bhebhe (2015), Dube (2011), Mutsagondo and Chaterera (2014) and Ngoepe (2017) as indicated in the literature review also criticise the Act for its failure to provide clear clauses on creation, storage, appraisal, destruction and transfer of digital records from records management systems to a digital archival repository. This may explain why there are loud calls from scholars like Matangira (2016:218) for the revision of the current NAZ Act to directly incorporate digital records management and preservation and to put provisions for designing of digital records management and preservation systems.

Carrying out digital preservation without conforming to standards as the studied departments were doing works against the sustainability of digital repositories. The use and development of standards has long been a cornerstone of the information industry since they facilitate access, discovery and sharing of digital resources as well as their long term preservation (DPC 2016b). Using standards that are relevant to the digital institutional environment helps with organisational compliance and interoperability between diverse systems within and beyond the sector (DPC 2016b). One such standard is the OAIS model which is an international standard (ISO 14721:2003). The model or standard identifies processes and functions common to almost every possible digital preservation environment (Gracy 2008:36). Adherence to standards also enables an organisation to be audited and certified.

The carrying-out of digital preservation without policies is also precarious. According to DPC (2016b), a digital preservation policy enables digital preservation to be carried out within an agreed framework and provides a clear line of responsibilities. The importance of an access and security policy also needs no over-emphasis. As noted by Asogwa (2012), databases containing personal, financial and medical records as observed in this research as well, can pose security, confidentiality and privacy violation challenges if proper access and security precautions are not put in place in the form of a policy. Lacking an ICT policy also poses great threat to the preserved records. As noted by Anie (2011), an ICT policy is an official statement which spells out the objectives, goals, principles and strategies among other things, intended to guide and regulate the development, operation and application of ICTs. The ICT policy in other words also ensures that an organisation's ICT related investment, operations and maintenance processes and usage are well directed for sustainability.

Paucity of retention and disposal policy in the studied departments is another indicator of faulty digital preservation in Masvingo province. There are therefore greater chances for loss of valuable records due to wrong disposal actions. This status quo also leaves chance for preservation systems to be clogged with records of ephemeral value and collapsing under their own weight. As earlier on highlighted in the literature review, a records retention and disposal policy prescribes requirements for the length of time a record must be retained and the appropriate means of disposal at the end of its life-cycle. It is one of the secrets for a successful preservation programme of any institution. Smith (2007) also argues that it is dangerous to think that an office can keep everything in digital form because if systems are upgraded, it may not be easy to migrate the information to new software. It is therefore not recommended to delay digital disposal of time-expired records.

Under the present situation in terms of the legal, standards and policy guidelines, Masvingo province is far from having sustainable digital preservation strategies and vital digital records may continue to be lost. Similar to the findings of this study, Bhebhe (2015) and also Nkala, Ngulube and Mangena (2012) observe that the execution of ICT based projects in Zimbabwe is done in a piece-meal approach without any policy, strategy and framework of principles to support the creation, maintenance and preservation of digital records and archives. Matangira (2016:197) also notes the lack of guidelines in most ministries in Zimbabwe. This study also confirms several studies of a similar nature in the ESARBICA region. For instance, Motupu (2015) notes the lack of digital records management policy in Botswana and Wamukoya and

Lowry (2013) note the lack of policies in Kenya and Uganda. These results are also in line with those of Nengomasha (2009) who discovers that the management of digital records in Namibia was highly challenged by lack of records retention and disposal policies, poor security and confidentiality controls as well as absence of policies and procedures to guide the management of both paper and digital records.

5.4 Infrastructure, resources and tools for digital preservation

The intended benefits of electronic government are compromised unless there is adequate infrastructure for managing and preserving the created digital records (Nkala, Ngulube and Mangena 2012:110). Storing records and archives in appropriate buildings, monitoring and controlling temperature, humidity and light are key to safeguarding records and archives (Ngulube 2003:289). As shown in Table 4.6 and 4.13 of Chapter Four, the infrastructure and resources the departments have are not adequate to sustain long-term digital preservation strategies. The province lacked purpose built records storage rooms or facilities with humidity and temperature controls, smoke detectors and dust filters or suckers. They also lacked cold room facilities. This state of affairs is not ideal if Masvingo province is to have effective digital preservation strategies. Dust can damage servers and lack of smoke detectors and adequate fire fighting equipment in the departments put records at greater risk in the event of fire outbreak. Stressing on the importance of appropriate infrastructure, Ngoepe and Van der Walt (2009) argue that a good policy and legal framework does not help much if there is no capacity to implement it and sound infrastructure to ingest archival digital records.

Uncontrolled environmental conditions are detrimental to digital records especially those on external storage media like CDs and DVDs. Although researchers are not in consensus about the suitable temperature and relative humidity levels that support long term preservation of digital records, DPC (2016b) suggests that temperature of around 20^0C and relative humidity of about 40% can be suitable for mixed collections. Controlled temperature and relative humidity environment also prolongs the life expectancy of external storage media. DPC (2016b) adds that the life expectancy of both CDs and DVDs is predicted to range from approximately two years at temperature of 28^0C and relative humidity of 50% to seventy-five years at a temperature of 10^0C and relative humidity of 25%.

The systems the departments were using were not conforming to the OAIS reference model which is also an ISO standard and a benchmark of preservation work. The systems were also not fully developed to allow for interoperability in the event of a change in the hardware and software environment. While it is justifiable that NAZ is not giving the departments adequate advice in the management and preservation of digital records (see Appendix vi), the departments are also to blame. This research established that the departments were carrying out digital preservation without adequate power supply and power backup. This is another big threat to the survival of digital records and the implementation of effective strategies for preservation of digital records in Masvingo province. According to the Minnesota History Society (2012), appropriate and sufficient power supply must be delivered to the server room because inadequate power causes servers to overheat and fail and loss of data is inevitable.

Insufficient budgets or lack of budgets as highlighted in Chapter Four of this study is another big factor militating against achieving sustainable strategies for preservation of digital records in Masvingo province. IT officers were complaining that they were lacking funds to purchase software packages, for system maintenance as well as for continuous training. On the other hand, records management officers were complaining that their section was the least prioritised when it comes to resources and funds allocation. It is therefore difficult under these circumstances for Masvingo province to implement comprehensive digital preservation strategies. According to Ngulube (2003:288), funding is key to formulating and implementing preservation programs. As earlier on highlighted in the literature review in Chapter Two, there are a number of costs associated with digital preservation like costs of programme and project management, skills training for staff and new software needed to implement the retention of digital records. Therefore, operating without a budget translates to futile endeavours in as far as preservation of digital records is concerned.

The findings of this study whereby the available infrastructure and resources were inadequate to support the long-term strategies for preservation of digital records in Masvingo province confirm Matangira (2016)'s observations that Zimbabwe is far from complying with the expectations of the records management standard ISO 15489-1:2001. The standard prescribes that facilities should be in place to ensure the capture and management of records in all formats through-out their life-cycle. A similar study by Ngulube (2012) where he was looking at preserving public digital information for the sustenance of e-governance in sub Saharan Africa also established that infrastructure in the greater part of sub-Saharan Africa is not adequate for

capturing, managing and preserving digital records including those on social media. In Tanzania, Lowry (2012) also notes that the ministries and departments creating the digital records lacked the facilities needed to store and preserve them reliably over time.

5.5 Professional knowledge and skills levels of staff

In today's digital environment, the focus is on capabilities to manage digital information in all systems where it is created, transmitted, managed, preserved and accessed (National Archives of Australia 2017). All the participants in this study had professional qualifications ranging from certificate level to masters level as shown in Tables 4.7; 4.8 and 4.9 in Chapter Four.

However, the administration officers had no qualifications inclined to records and archival management. This may partly explain the inadequate management support to the needs of the records management sections. However, on the other hand, the responses of the records management officers also point to the weaknesses in the training they received. Although all the records management and IT officers had qualifications inclined to their duties, they largely appeared to be novices in the area of digital preservation. Their lack of knowledge about the OAIS digital preservation model and digital repository audit criteria is a clear indication that the ineffectiveness of the digital preservation strategies Masvingo province is currently using may be a product of the failure by those charged with the preservation responsibility to adequately present to management the exact requirements for digital preservation. As put across by ICA (2016), the OAIS reference model and the digital repository audit method based on risk assessment (DRAMBORA) provide terminology and knowledge in planning infrastructure and resources that accounts for all aspects of the digital records preservation process.

The findings of this research showed that departments C, F, H, I, J and M have bestowed the preservation of their digital records on IT officers. However, as NECCC (2004) would argue, the arrangement is not very ideal since these officers had no knowledge of what systems and rules are needed to ensure that the records are captured and maintained, how long they should be kept to meet business and other requirements and how they should be stored. IRMT (2003) shares similar sentiments and argues that IT specialists tend to focus primarily on current information needs resulting in inadequate attention being paid to long-term preservation requirements. This partly explains why ingestion of digital records was not given thorough

attention as required by the OAIS reference model which provided this research with a conceptual framework. The preservation of digital records in Masvingo province is therefore marred with a lot of flaws as there are no submission agreements between the creators of the records and those charged with their preservation and records were not packaged into SIPs. There was also no validation system to verify the integrity, completeness and correctness of records at ingestion stage.

Records management officers confessed that the curriculum they studied was more inclined to the management and preservation of paper records with little depth on management and preservation of digital records. The records management and IT officers also highlighted that their departments were neither prioritising staff development nor sending them for seminars, conferences and workshops. Consequently, in Masvingo province most of the records management and IT officers' professional knowledge and skills levels appeared to have been out-paced by technological developments. Their lack of trust in the digital preservation system which resulted in most of them to resort to printing and filing some of their digital records can therefore be attributed to lack of both adequate resources as well as a dearth of practical technical skills to execute sustainable digital preservation strategies.

The findings of this research are similar to the observations of Malemelo, Dube, David and Ngulube (2013) who note that computer systems at Marondera Municipality were not being extensively used in the day to day activities and members of staff were not well versed with some information technology programs used in financial records management. Similarly, Matangira (2016) argues that the issue of basic training in records is no longer the biggest problem in Zimbabwe but the type of training. She adds that the training is weak in equipping graduates with skills to use ICTs in records management. Nengomasha (2013:7) also notes that the developments in records and archives training in sub Saharan Africa have not done much to improve records keeping in organisations. Wamukoya and Lowry (2013) also note that Kenya, Uganda and Tanzania do have professional archivists as well as training institutions for capacity building but lack the digital aspect as they focus more on paper records.

5.6 Access, security and privacy issues

Preservation strategies are bound to be ineffective if proper access, privacy and security issues are not addressed to guard the collection against malicious damage, loss, forgery and theft, and to ensure that files are presented according to user needs (Gracy and Kahn 2012). As also highlighted in the literature review, records preservation systems should include and apply controls on access to ensure that authenticity, integrity, reliability and accessibility properties of records are not compromised (ISO 15489-1 2001:10). It is a common notion that if a record is not authentic, there is no need to preserve it (Milton 2000). Access, security and confidentiality or privacy controls support digital preservation strategies and programmes. Furthermore, they give an understanding of who has access to content, who can perform what actions on that content and enforcing these access restrictions (DPC 2017).

This research found out that access to preserved digital records in the studied public departments in Masvingo province was online. Authentication and authorisation were the methods used to technically protect records from unauthorised access and tempering. Users of records were having access rights that correspond to their duties. However, this research also found out that Masvingo province was yet to thoroughly deal with access, privacy and security issues since all the departments were operating without access policies, digital records disaster management plans and guidelines for managing digital storage media.

This situation is not ideal for digital preservation strategies to yield continued access to records. An access policy is critical in all preservation efforts because it is developed with sensitivity to strike a balance between the right to access information and protection of privacy. In addition to that, it ensures the safety of the record, compliance with legislation and archival practices and guarantees the existence of materials for future users (National Archives of St Kitts and Nevis 2011). Operating without an access policy makes preservation of digital records unsustainable. It also exposes organisations to adverse effects of litigation due to greater likelihood of infringement of privacy and confidentiality issues.

Since digital storage systems are prone to disasters, operating without a disaster management plan as the studied departments were doing, poses great risk of losing completely the preserved records. A disaster management plan is critical as far as continued access to digital records is concerned because it provides detailed instructions for staff to follow in the event of different

types and scales of disaster. Additionally, it provides instructions for restoring the content of the digital collection from backup copies among other things (IRMT 2009). Lack of guidelines for handling storage media as was the case in the studied departments is also another quick recipe for digital records to become irretrievable.

The departments that had social media accounts were also lacking guidelines pertaining to the use of such records. As also indicated in Chapter Four, the departments admitted that they were facing challenges to access some of their records due to poor arrangement, description and indexing as the records were just stored without adequate metadata. Above all, the departments were also ignorant about other access legislations in Zimbabwe like AIPPA. At department C, the client computers were inadequate to the extent that officers were sharing. This was giving chance for unauthorised access when the authorised officer forgets to sign-out. This shows that at the present moment, departments in Masvingo province were yet to strike a balance between access to and overall security of the stored digital records.

These short-comings are detrimental to the survival of digital records and for continued access to them. The situation also makes it difficult for preservation strategies to be effective. As highlighted in the introduction of this study in Chapter One, there is a strong link between preservation and access and the major objective of preserving the information content is to make it accessible to both current and future generations.

Inadequate attention to access, security and privacy issues has seen the Masvingo province facing numerous challenges that were indicated in Table 4.10 of Chapter Four. The challenges include hacking, viruses, crushing of machines, deletion of files and unauthorised access. Although the challenges were yet to be rampant as shown in Table 4.8, they have the potential to cause unprecedented loss of valuable digital records in the province. Necessary steps to mitigate their effects must be considered as a matter of agency. The slightly lower prevalence of these challenges at the moment maybe due to the fact that all the departments were running hybrid systems of both paper and digital records. However with the projected exponential increase in the generation of digital records alluded to in the introduction in Chapter One, these challenges if not addressed are bound to become widespread leading to more loss of records.

Poor security and confidentiality controls have also been identified as major factors contributing to the failure in capturing and preservation of digital records in the ESARBICA region (Wamukoya and Mutula 2005).

5.7 Summary

Some of the digital records departments in Masvingo province preserve are of enduring value and sensitive. The records needed long-term preservation strategies and proper access, security and privacy controls to guarantee continued access to them. However, the strategies the departments were using to preserve them at the moment were makeshift and interim in nature. Available infrastructure, resources, budgets and skills levels were yet to be commensurate with the requirements for long-term digital preservation outlined in the OAIS reference model. Lack of supporting legal framework, policies, standards and guidelines was another factor making the strategies for preservation of digital records in Masvingo province to fail to guarantee long-term access to these resources. The departments were also battling it alone without guidance from NAZ which also lacks expertise and infrastructure to ingest their records. The province was also yet to strike a balance between access to and overall security of their digital records. Preservation of digital records in Masvingo province is therefore an on-going struggle. The next chapter summarises and concludes the study. It also makes recommendations on how public departments in Masvingo province can improve the preservation of their digital records.

CHAPTER SIX
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter serves as a concluding part of the study findings that were presented in Chapter Four and their interpretation and discussion presented in Chapter Five. The chapter ties together the various issues raised in the body of the study and makes comments upon their meaning (Assan 2006:1). This chapter is invaluable as it shows how the study achieved its objectives and answered the research question (Jokonya 2014:188). The chapter is also important because it assesses the study in terms of its contributions to the body of knowledge. In light of this, the chapter has been structured to include the summary, conclusions, recommendations, suggestions for further research, and implications for theory, policy and practice. The summary and conclusions were drawn from the objectives, research questions and findings of the study. Recommendations were based on literature review presented in Chapter Two and the interpretation and discussion of the study findings presented in Chapter five.

6.2 Summary

This study was undertaken to investigate the strategies for preservation of digital records in Masvingo province of Zimbabwe. The main problem this study seeks to address is that, public departments in Masvingo province are losing significant digital records that should be strengthening their accountability, transparency and effectiveness in delivering their core mandates. The OAIS reference model was used as the conceptual framework of this study. The study used a qualitative research approach and adopted a multiple case study design to address the research questions. The study investigated digital preservation strategies in thirteen departments that were generating and preserving digital records in the province. Participants in this study were purposively selected due to their involvement in the management, preservation and use of digital records. Data was collected using face to face interviews, observation and document analysis. Furthermore, data was manually processed and analysed using thematic content analysis.

This research established that some of the records classes and file types as shown in Tables 4.2 and 4.3 respectively in Chapter Four, that the case study departments were preserving are of enduring value and sensitive. The records require long-term preservation and proper security protection. The departments were using backup and byte replication, migration, printing and filing, capturing preservation metadata and cloud computing strategies to preserve their records as shown in Table 4.5 in Chapter Four. However, these strategies were not chosen because they were the best for the types of digital records preserved. They were simply adopted because those charged with the preservation of the digital records have limited skills and knowledge. Besides that, the available infrastructure was not suitable and the resources for digital preservation were inadequate.

Some of the strategies like backup and byte replication are only suitable for short-term to mid-term strategy to extend the life of digital records. The departments were also yet to embrace open standard and non-proprietary formats in their migration efforts and hence they were very vulnerable to losing information through technological obsolescence. Some departments were ignorant about simple basics of preservation like capturing metadata and the officers lamented that they were having a torrid experience in accessing the stored records. Printing and filing was also proving meaningless for some file types such as video and audio as well as those with multiple links. Above all, all the studied departments were yet to use TDRs that can manage digital resources to their designated community now and in the future and are OAIS compliant. The departments were also lacking knowledge about preservation softwares such as AtoM and Archivematica that are compliant to archival standards like the OAIS reference model. Participants were also ignorant about preservation assessment toolkits like TRAC, NESTOR and DRAMBORA as well as software tools like DSPACE, FEDORA, LOCKSS and DAITSS that are crucial for generation of technical metadata to support the preservation of digital records.

The strategies the province is using are also failing to guarantee long term access to the digital records due to lack of strong legal framework. The legal framework which is the NAZ Act of 1986 was not giving the creating agencies much help as it does not have specific clauses on the creation, appraisal, preservation and destruction of digital records. All the departments were not conforming to digital preservation standards despite them being the cornerstone of the information industry. Furthermore, they also facilitate access, discovery and sharing of digital resources as well as their long term preservation (DPC 2016b). The departments were also

lacking preservation policies, security and access policies and guidelines for selecting records for preservation as well as for handling storage media. Although some few departments had ICT and retention and disposal policies, the documents were in need of review to include much on management, preservation and disposal of digital. Digital records in Masvingo province are therefore prone to loss and the departments are at the verge of experiencing more access, security and privacy challenges. This lack of a supportive legal framework, policies, standards and guidelines was a shared blame between NAZ and the records creating agencies.

The infrastructure and resources the departments in Masvingo have were not adequate to sustain long-term digital preservation strategies. The province lacked purpose built records storage rooms with humidity and temperature controls, smoke detectors and dust filters. The systems the departments were using were also not fully developed to allow for interoperability in the event of changes in the hardware and software environment. Other departments were also lacking power backup kits thus exposing their servers to overheating, failure and inevitable loss of data. It was again sad to note that the departments were operating with inadequate budgets or no budget at all. There were louder cries that the records management section was the least priority in terms of resource allocation. This was a major setback for these departments to execute sustainable digital preservation strategies. By and large, departments were failing to meet costs associated with digital preservation like cost of programme and project management, skills training for staff and new software packages needed to implement the long-term preservation of digital records.

Although all the participants in this study had qualifications ranging from certificate to masters level, there was a great disparity between the qualification on paper and what the holder of the qualification can perform in as far as digital records preservation is concerned. The highest qualifications were observed amongst the top administration officers but unfortunately they were not inclined to records and archival management. The records management and IT officers had qualifications inclined to records management and preservation but were ignorant about issues that matters most in preservation of digital records such as standards, metadata schemas, policies and guidelines as well as software that are archival compliant like Archivematica. Selection of digital records for preservation was not done properly due to lack of appraisal skills. Ingestion of digital records for preservation was not done according to the dictates of the OAIS reference model. Most records management officers confessed that the

records management curriculum they studied was more inclined to the management and preservation of paper records with little depth on digital records.

Access to the preserved digital records was online and authentication and authorisation procedures were used to protect records from both unauthorised access and tempering. However the province was yet to thoroughly deal with access, privacy and security issues. The departments were also ignorant about the bearing of other legislations like AIPPA on access. Inadequate attention to access, security and privacy issues saw the province encountering challenges like hacking, viruses, crushing of machines and unauthorised access as shown in Table 4.10 in Chapter Four.

6.3 Conclusions

This section presents the conclusions derived from the study. It is arranged in line with the research questions of the study.

6.3.1 Strategies for preservation of digital records

The strategies for preservation of digital records in Masvingo province are compromising the long-term preservation and security of these resources. The strategies are at the moment makeshift and interim in nature as they cannot be trusted to guarantee continued access to the stored digital records. The ineffectiveness of the strategies the province is using is a shared blame between NAZ and the records creating agencies. On one hand, the creating agencies put up their digital preservation systems without consulting NAZ. On the other hand, NAZ has not only left the role of preserving digital records to these creating agencies, but is also not giving them adequate guidance and advice as required by the NAZ Act (see Appendix vi). Under the present situation, there is room for Masvingo province to continue losing more information.

6.3.2 Legal, standards and policy guidelines

The digital preservation scenario in Masvingo province appears much to be at its infancy stages and the preservation strategies are implemented in an *ad-hoc* fashion due to lack of sound legal, standards and policy guidelines for preservation of digital records. Lack of these controls and guidelines is militating against the establishment of sustainable digital repositories

in Masvingo province of Zimbabwe. At the moment, there are no checks and balances to guarantee continued access to digital records and standard benchmarks that can lead to effectiveness of the digital preservation strategies in Masvingo province. Digital preservation is therefore not carried out within an agreed framework with clear lines of responsibilities. This situation also leaves greater chances for loss of valuable digital records due to wrong disposal actions and clogging of the preservation infrastructure with records of questionable and ephemeral values. NAZ is also to blame for failing to come up with both a better legislation or preservation policy and guidelines for creation, management, appraisal, preservation and disposal of digital records.

6.3.3 Infrastructure, resources and tools for digital preservation

The infrastructure and the resources the departments have are not adequate to sustain long-term digital preservation strategies. Records are in danger of becoming irretrievably lost due to storage in an environment where temperature and humidity are not controlled and in servers exposed to dust and inadequate power supply. Lack of budgets in most departments for preservation activities buttresses the view that records and archival management is looked down upon by top administration in Masvingo province. The current infrastructure and resources situation in Masvingo province suggests that a thorough cost benefit analysis and digital readiness assessments were not done before departments started preserving digital records. Consequently, at the present moment digital preservation in Masvingo province of Zimbabwe is yet to be fully developed.

6.3.4 Professional knowledge and skills of staff

The officers charged with the preservation of digital records in Masvingo province are more conversant with the preservation of paper records than the digital ones. Their skills and knowledge levels is greatly limiting them to implement viable strategies for preservation of digital records. Preservation of digital records is at the moment done in an *ad-hoc* and piece-meal fashion. Understanding of digital preservation among members of staff who participated in this research was shallow owing to their ignorance about the OAIS reference model which is a common reference point for building understanding and consensus, and for advancing the objectives of digital preservation and interoperability. Without adequate technical expertise as is the case at the moment, the development of preservation of digital records in Masvingo is in

limbo. With the lack of appraisal and ingestion skills noted in this study, digital preservation strategies in Masvingo province are bound to be unsustainable.

6.3.5 Access, security and privacy issues

The province is yet to thoroughly deal with access, privacy and security issues. The departments are operating without access policies, ICT policies, digital records disaster management plans and guidelines for managing storage media. Departments are therefore bound to lose more records and to fail to ensure accountability, transparency and improved service delivery. The departments are also at risk of suffering the adverse effects of litigation due to negligence on issues of privacy and confidentiality.

6.4 Recommendations

Strategies for preservation of digital records in Masvingo province have been established as well as the factors militating against continued access to these resources. In this section, the researcher proffers recommendations for improved preservation of digital records in the province.

6.4.1 Strategies for preservation of digital records

Departments should consider using TDRs which can manage digital resources to their designated community now and in the future and are OAIS compliant. TDRs can be audited to ensure appropriate performance and quality management with assessment toolkits like TRAC, NESTOR, and DRAMBORA among others. They also work well with software tools for digital preservation like AtoM and Archivematica among others. Modelling preservation strategies in line with the OAIS reference model is crucial because the model provides a framework for digital preservation plans, strategies and initiatives. The model is also an approved ISO standard that is currently considered the benchmark for digital preservation system (ICA 2016). It addresses all aspects of long-term preservation of digital information, that is, ingest, archival storage, data management, access, dissemination and migration to new media and forms (Ngoepe 2017).

The departments should make sure that their preservation systems capture all forms of metadata, that is, technical, management and discovery metadata. Metadata is invaluable for guaranteed preservation, rendition, authenticity, easy location, access and use of digital records.

The departments should also strive to perform migration by normalisation. This strategy involves the migration of the data file to standard open source format that is always available, accessible and promotes interoperability between differing systems. This reduces the number of digital formats and costs of regular migrations thereby promoting the sustainability of digital preservation. Other tried and tested archival non-proprietary formats such as PDF/A may also be considered for use to prolong the life of digital records that can be converted into such formats.

The departments should explore for adoption, the use of Application Programming Interfaces (APIs) for harnessing and preservation of social media and website content. The use of cloud storage for less sensitive information may also be considered as a viable and cost effective interim strategy for use by both NAZ and the records creating departments to reduce pressure on the inadequate preservation infrastructure. Above all, there should be a closer cooperation and working together between records creating agencies, IT experts and NAZ for improved digital preservation strategies.

6.4.2 Legal, standards and policy guidelines

The current NAZ Act which is the legal framework for the management and preservation of digital records should be amended to give adequate and specific guidelines for the management and preservation of digital records. Alternatively NAZ should come up with a digital preservation policy and guidelines that augment the Act for the departments to follow as they execute digital preservation. A policy on distributed custody may also be desirable at the moment to give creating agencies the mandate to preserve digital records until such a time when NAZ is able to ingest digital records from public sector departments.

All digital preservation strategies and activities should conform to standards for sustainability and effectiveness. Adhering to standards such as ISO 15489-1:2001, ISO 14721:2012, ISO 31000:2012, ISO/IEC 27001:2013, and ISO/TR 18492:2005 described in the literature review

in Chapter Two and other relevant ISO standards is most recommended for preservation efforts to be in line with global trends and best practices.

The departments should come up with other documents such as the ICT, retention and disposal, and access policies as well as disaster management plans. These instruments are crucial for digital records preservation strategies and activities to be executed in compliance with legislations and archival practices to guarantee the existence of digital materials for future use. NAZ should be proactive in auditing public departments on the availability of these instruments and ensuring that those having challenges in coming up with them are assisted accordingly.

6.4.3 Infrastructure and resources

The departments in Masvingo province should consider having special rooms for storage of digital records with controlled temperature, humidity, dust and sunlight for proper working of servers and long-term storage and survival of external storage media. Substantial budgets should also be put in place to support digital preservation activities.

Top management should also change their mind-set and start to consider records and archives management as key to service delivery and start to prioritise this sector in resource allocation. The infrastructure and resources crisis in Masvingo province is a wakeup call for the Government of Zimbabwe to capacitate NAZ to come up with provincial and national data centres to ingest digital records from public sector departments for future use.

6.4.4 Professional knowledge and skills

Substantial investment should be channelled towards improving staff skills in digital records management and preservation. The departments should consider funding continuous training of staff through workshops, conferences, short courses and college or university programmes with more emphasis on the practical side of digital preservation. All the relevant stakeholders, that is, records creating agencies, the academia, NAZ and the government, should come together and consider revising the records and archives curriculum. Furthermore, they should work towards equipping tertiary institutions with TDRs and other necessities that will give hands on

experience and technical skills to students for them to be able to deal with digital preservation challenges at the work place.

6.4.5 Access, security and privacy issues

Access, security and privacy issues should be thoroughly addressed through policies. The physical infrastructure and the computer systems should be tightly protected to inhibit unauthorised access, alterations and viral attacks to information.

6.5 Suggestions for further research

This study examined the strategies for preservation of digital records in Masvingo province of Zimbabwe. The study managed to give a picture of the factors militating against effective preservation of digital records in Masvingo province by including in the examination a scrutiny of the legal, standards and policy guidelines; infrastructure and skills requirements; security, privacy and access issues; as well as giving recommendations that can improve the preservation of digital records in the province. NAZ and private sector departments were out of the scope of this study.

Therefore, the researcher is firstly recommending separate studies looking at the management of public sector digital records to be carried out so as to add background and depth into understanding the digital preservation challenges Masvingo province is currently facing. Secondly, separate studies to investigate NAZ's position in as far as the preservation of public digital records is concerned should also be carried out. This may shed more light into the direction and steps the government and NAZ are taking to address the digital conundrum in Zimbabwe. Thirdly, the researcher is suggesting that studies to investigate management and preservation of digital records in the private sector should also be carried for comparison purposes with studies in the public sector like this current one. This will give deeper and broader insights into digital records management and preservation in Masvingo province and Zimbabwe at large.

Fourthly, this study only looked at public departments scattered in the provincial capital and so, the researcher is also recommending studies that will spread wings to include digital records management and preservation experience in all the districts of the province. This will

give a thorough reflection of the digital records preservation strategies in Masvingo province. Last but not least, Masvingo is just one province in a country with ten administrative provinces. The researcher is therefore suggesting that researches examining digital records management and preservation in Zimbabwe as a whole should be carried out for more robust reflection of digital records management and preservation in Zimbabwe.

6.6 Implication for theory, policy and practice

The findings of this study confirm results of other researchers like Nengomasha (2009), Ngulube (2012), Nkala, Ngulube and Mangena (2012), Nengomasha (2013), Wamukoya and Lowry (2013), Mutsagondo and Chaterera (2014), Bhebhe (2015), Moputu (2015), Matangira (2016) and Ngoepe (2017). The difference between this study and these others is that it managed to explore a broader picture of the strategies for preservation of digital records in the public sector in Masvingo province using a multi-case study research design. Although the study built on the outcomes of the mentioned researchers, it managed to further contribute to knowledge in the field of digital preservation as it shows how the OAIS reference model can be used to build understanding and consensus in digital preservation and to advance the objectives of digital preservation and interoperability as a framework for digital preservation plans, strategies and initiatives.

It is hoped that the recommendations of this study can form invaluable building blocks for revising the NAZ Act or in coming up with a comprehensive digital preservation policy. Furthermore, the recommendations can be vital for crafting instruments like the ICT policy that Masvingo province and Zimbabwe at large desperately need. This study may perhaps contribute to the wider adoption and use of the OAIS reference model in the designing implementation and evaluation of digital preservation systems in Masvingo province and Zimbabwe at large.

6.7 Final conclusion

The strategies for preservation of digital records in Masvingo province are failing to guarantee long-term preservation and security of these resources. This is due to lack of supportive legal, standards and policy guidelines, budgets and skilled manpower. Other reasons include inadequate infrastructure, unconducive storage environments and poor working relationship

between top management, records preservers, IT experts, academia and NAZ. The strategies for preservation of digital records are therefore executed in an *ad-hoc* fashion. The strategies used are also interim in scope. There is therefore an urgent need to address these flaws and shortcomings in a more collaborative effort to curb the continued loss of digital records that are invaluable for accountability, transparency, informed decisions and improved service delivery among other things.

REFERENCES

Adu, KK. 2015. Framework for digital preservation of electronic government in Ghana. PhD thesis, University of South Africa, Pretoria.

Akotia, P. 2000. The management of public sector financial records: implications for good government. *African Journal of Library, Archives and Information Science* 10(2):167-175.

Anderson, C. 2010. Presenting and evaluating Qualitative research. *American Journal of Pharmaceutical Education* 74(8):1-7.

Anie, SO. 2011. The economic and social benefits of ICT policies in Nigeria. Available at: http://digitalcommons.unl.edu/cgi/viewcontent.cgi%3Farticle%D1475%26context%3Dllibphilprac&sa=U&ved=0ahUKEwjG6o3c0pLWAhWROsAKHUp-ADcQFggIMAA&usg=AFQjCNHoPCPGVqk_O0szYMqinFOiVJLGhA (Accessed 29 June 2017).

Asogwa, BE. 2012. The challenge of managing electronic records in developing countries: implications for records managers in sub-Saharan Africa. *Records Management Journal* 22(3):198-221.

Asproth, V. 2005. Information technology challenges for long-term preservation of electronic information. *International Journal of Public Information Systems* 2005(1):27-37.

Assan, J. 2006. Writing the conclusion chapter: the good the bad and the missing. Available at: http://www.devstud.org.uk/downloads/4be165997d2ae.pdf (Accessed 16 August 2017).

Babbie, E. 1990. *Survey research methods.* 2nd edition. California: Wadsworth Publishing Company.

Babbie, E. 2004. *The practice of social research.* 10th edition. Southbank Victoria: Wadsworth Thompson.

Babbie, E. 2010. *The practice of social research.* 12th edition. Belmont: Cengage Learning Inc.

Babbie, E. 2011. *The basics of social research.* 6th edition. Wadsworth: Cengage.

Barateiro, J, Antunes, G, Freitas, F & Borbinha, J. 2010. Designing digital preservation solutions: a risk management based approach. *International Journal of Digital Curation* 5(1):4-17.

Barve, S. 2007. File formats in digital preservation in Prasad, A.R.P and Madalli, D.P (eds), *ICSD-2007*:239-248. Available at: http://dlissu.pbworks.com/f/file%2Bformat1.pdf (Accessed 23 August 2016).

Baxter, P & Jack, S. 2008. Qualitative case study methodology: study design and implementation for novice researchers. *The Qualitative Report* 13(4):544-559.

Begum, RA. 2015. Preserving social media: a case of LTU archives. Masters' thesis, Lulea University of Technology, Lulea.

Bernard, HR. 2000. *Social Research methods: qualitative and quantitative approaches*. Thousand Oaks: Sage.

Bhattacherjee, A. 2012. Social science research: principles methods and practices. Available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi? (Accessed 29 August 2016).

Bhebhe, S. 2015. Contemporary diplomatics of the civil and deceased estate case files found at the National Archives of Zimbabwe. *Records Management Journal* 25(1):107-120.

Billups, F. 2014. The quest for rigor in qualitative studies: strategies for institutional researchers. Available at: https://www.airweb.org/eAIR/specialfeatures/Documents/ArticleFBillups.pdf (Accessed 29 October 2016).

Blaike, N. 2010. *Designing social research.* 2nd edition. Cambridge: Polity Press.

Bobbie, L. 2007. Sampling: What is it? Available at: http://webpages.acs.tt.edu/rlatham/Coursework/5377(Quant)/Sampling_Methodology_Paper.pdf (Accessed 24 October 2016).

Branco, TT & Santos, H. 2015. A trust model for cloud computing environment, in *Proceedings of the 3rd Conference on Cloud Security and Management ICCSM-2015*, edited by BE Popovsky. Washington: Academic Conferences and Publishing International Limited: 1-15.

Brown, PA. 2008. A review of the literature on case study research. *Canadian Journal for New Scholars in Education* 1(1):1-13.

Bryman, A. 2004. *Social research methods.* 2nd edition. Oxford: Oxford University Press.

Bryman, A. 2008. *Social research methods.* 3rd edition. Oxford: Oxford University Press.

Cain, P & Thurston, A. 1998. *Personnel records: a strategic resource for public sector management.* London: IRMT.

Campbell, R & Ahrens, CE. 1998. Innovative community services for rape victims: an application of multiple case study methodology. *American Journal of Community Psychology* 26(4):537-571.

Chaleunvong, K. 2009. Data collection techniques. Available at: http://www.gfmer.ch/Activities_internationales_Fr/Laos/PDF/Data_collection_techniques_Chaleunvong_Laos_2009.pdf (Accessed 26 October 2016).

Chaterera, F. 2012. Towards harnessing e-government adoption in Zimbabwe. *Mousaion* 30(2):78-93.

Chaterera, F. 2013. Records surveys and the management of public records in Zimbabwe. M lnf dissertation, University of South Africa, Pretoria.

Chaterera, F. 2016. Managing public records in Zimbabwe: the road to good governance, accountability, transparency and effective service delivery. *Journal of the South African Society of Archivists* 49:116-136.

Chaterera, F, Ngulube, P & Rodrigues, A. 2014. Records surveys in support of a framework for managing public records in Zimbabwe. *Information Development* 30(4):366-377.

Chaturvedi, K. 2016. Sampling methods. http://www.pitt.edu/~super7/43011-44001/43911.pdf Available at: (Accessed 24 October 2016).

Cohen, DCB. 2006. *Qualitative research guidelines project.* College Road East: Robert Wood Johnson Foundation.

Consultative Committee for Space Data System (CCSDS). 2012. *Recommendation for space data system practices – Reference model an Open Archival Information System OAIS – Recommended Practice CCSDS 650.0-M-2.* Washington (DC): CCSDS.

Coontz, P. 2008. The responsible conduct of social research, in Yang, K & Miller, GJ (eds), *Handbook of research methods in public administration*. Boca Raton: Taylor and Francis Group: 129-140.

Corrado, EM & Moulaison, HL. 2014. *Digital preservation for libraries, archives and museums*. Lanham: Rowman & Littlefield.

Creswell, JW. 1998. *Qualitative inquiry and research design: choosing among five traditions.* Thousand Oaks: Sage.

Creswell, JW. 2009. *Research design; qualitative quantitative and mixed methods approaches*. 3rd edition. Los Angeles: Sage.

Creswell, JW. 2014. *Research design; qualitative quantitative and mixed methods approaches*. 4th edition. London: Sage.

Cunningham, A. 2011. Ghosts in the machine: towards a principles-based approach to making and keeping digital records, in Lee, CA (ed), *I, digital: personal collections in the digital era.* Chicago IL: Society of American Archivists: 78-89.

Curry, LA, Nembhard, IM & Bradley, EH. 2009. Qualitative and mixed methods provide unique contributions to outcomes research. *Circulation* 119:1442-1452.

Denzin, NK & Lincoln, YS. 2000. *Handbook of qualitative research.* 2nd edition. London: Sage.

Digital Preservation Coalition (DPC). 2014. The Open Archival Information System (OAIS) Reference Model: Introductory guide. 2nd edition. Available at: http://www.dpconline.org/component/domain/doc_download/1359-dpctw14-02 (Accessed 27 August 2015).

Digital Preservation Coalition (DPC). 2016a. Preserving social media: DPC Technical Watch Report 16-01 February 2016. Available at: http://handbook.dpconline.org/docman/technology-watch-reports/1486-twr16-01-1.pdf (Accessed 24 May 2016).

Digital Preservation Coalition (DPC). 2016b. Standards and best practice. Available at: http://handbook.dpconline.org/institutional-strategies/standards-and-best-practice (Accessed 26 August 2016).

Digital Preservation Coalition (DPC). 2017. Information security. Available at: http://www.dpconline.org/handbook/technical-solutions-and-tools/information-security (Accessed 16 August 2017).

Dobratz, S, Schoger, A & Strathmann, S. 2007. The nestor catalogue of criteria for trusted digital repository evaluation and certification. Available at: https://journals.tdl.org/jodi/index.php/jodi/issue/view/34 (Accessed 13 September 2016).

Dube, T. 2011. Archival legislation and the challenge of managing archives in Zimbabwe. *ESARBICA Journal* 30:279-290.

Duranti, L. 2005. The long-term preservation of accurate and authentic digital data: the InterPARES project. *Data Science Journal* 4(25):106-118.

Duranti, L. 2010. Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. *Records Management Journal* 20(1):78-95. Available at: http://dx.doi.org/10.1108/09565691011039852. (Accessed 25 February 2016).

Egwunyenga, E. 2009. Records keeping in universities: associated problems and management options in South West geographical zone of Nigeria. *International Journal of Education and Science* 1(2):109-113.

Elmusharaf, K. 2012. Qualitative data collection techniques. Available at: http://www.gfmer.ch.SRH-Course-2012/research-methodology/qualitative-data-collection-Elmusharaf-2012.htm (Accessed 9 June 2017).

Fielding, N & Thomas, H. 2008. Qualitative interviewing, in Gilbert, N (ed), *Researching social life*. London: Sage Publications.

Fink, A. 1995. *How to sample in surveys.* vol 6. London: Sage Publications.

Finn, J & Jacobson, M. 2008. *Just practice: a social justice approach to social work.* Peosta: Eddie Bowers Publishing.

Galloway, J & Sheridan, SM. 1994. Implementing scientific practices through case studies: examples using home-school interventions and consultation. *Journal of School Psychology* 32:385-413.

Ginsberg, W. 2013. Retaining and preserving federal records in a digital environmental: background and issues for congress. Available at: http://www.fas.org/sgp/crs/misc/R43165.pdf. (Accessed 12 June 2015).

Golafshani, N. 2003. Understanding reliability and validity in qualitative research. *The Qualitative Report* 8 (4):597-607.

Gracy, KF. 2008. Digital preservation basics: how to ensure long term access to your digital assets. Available at: http://norasis.slis.kent.edu/presentations/karenGracy/NORASIST_Dig_Pres_2008.ppt (Accessed 28 January 2016).

Gracy, KF & Kahn, MB. 2012. Preservation in the digital age. *Library Resources & Technical Services* 56 (1):25-43.

Guba, EG. 1981. Criteria for assessing the trustworthiness of naturalistic inquiries. *Education Communication and Technology Journal* 29:75-91.

Gumbo, L. 2016. Cyber crime bill: the details. *Herald Newspaper.*17 August 2016.

Hamooya, C, Mulauzi, F & Njobvu, B. 2011. Archival legislation and the management of public sector records in Zambia: A critical review. *Journal of the South African Society of Archivists* 44:116-123.

Hancock, B, Ockleford, E & Windridge, K. 2009. *An introduction to qualitative research.* Yorkshire: The NIHRRDS for the East Midlands.

Harding University. 2017. Chapter four: Data analyses and presentation of the findings. Available at: http://www.harding.edu/sbreezeel/461/chapter4a.pdf (Accessed 28 June 2017).

Harling, K. 2016. An overview of case study. Available at: http://www.farmfoundation.org/news/articlefiles/1028-1_harling.pdf (Accessed 25 October 2016).

Henry, GT. 1990. *Practical sampling.* vol 21. London: Sage Publications.

Hess, DR. 2004. How to write an effective discussion. *Respir Care* 49(10):1238-1241.

Hockx-Yu, H. 2014. Archiving social media in the context of non-print legal deposit. Available at: http://library.ifla.org/999/1/107-hockxyu-en.pdf (Accessed 28may 2016).

Hofman, H. 2006. Standards: not 'one size fits all'. *The Information Management Journal May/June* 2006:36-45.

International Council on Archives (ICA), 2016. *Digital preservation in lower resource environments core curriculum: understanding digital records preservation initiatives.* London: IRMT.

International Organisation for Standardisation (ISO). 2001. *ISO 15489-1 Information and documentation – records management-part 1general.* Geneva: ISO.

International Records Management Trust (IRMT). 2003. "*E-record readiness: Establishing electronic records as a component of electronic government", a proposal to the Common-wealth secretariat public sector information program.* London: IRMT.

International Records Management Trust (IRMT). 2004. *Evidence-based governance in the electronic age.* London: IRMT.

International Records Management Trust (IRMT). 2009. *Preserving electronic records: Training in electronic records management*. Module 4. Available at: http://www.irmt.org/documents/educ_training/term%20modules/IRMT%204.pdf (Accessed 06 August 2015).

International Records Management Trust (IRMT). 2011. *Managing records as reliable evidence for e-government, ICT, freedom of information: an east African regional situation analysis.* London: IRMT.

InterPARES/ICA. 2012a. Digital records pathways: Topics in digital preservation. Module1: Introduction –A framework for digital preservation. Available at: http://www.interpares.org/display_file.cfm?doc=ip3_canada_gs12_education-modules_digital-records-pathways.zip (Accessed 07 August 2015).

InterPARES/ICA. 2012b. Digital records pathways: Topics in digital preservation. Module 2: Developing policy and procedures for digital preservation. Available at: http://www.interpares.org/display-file.cfm?doc=ip3_canada_gs12_education-modules_digital-records-pathways.zip (Accessed 07 August 2015).

InterPARES/ICA. 2012c. Digital records pathways: Topics in digital preservation. Module 8: Cloud computing primer Introduction. Available at: http://www.interpares.org/display_file.cfm?doc=ip3_canada_gs12_education-modules_digital-records-pathways.zip (Accessed 07 August 2015).

InterPARES 3 Project Team Canada. 2013. General study 08-Open-Source Records Management Software: final report. Available at: http:/www.interpares.org/display_file.cfm?doc=ip3_canada_gs08_final_report.pdf (Accessed 08 July 2015).

Joint Technology Committee. 2014. Developing an electronic records preservation and disposition plan: version 1.0. *Resource Bulletin.* Available at: 20US/Committes/JTC/JTC%20Resource%20Bulletins/6JTC%20E%20Records%2010 %20FINAL.ashx (Accessed 10 June 2015).

Jokonya, O. 2014. A framework to assist organisations with information technology adoption governance. D Phil thesis, University of South Africa, Pretoria.

Kalusopa, T. 2011. Developing an e-records readiness framework for labour organisations in Botswana. D Phil thesis, University of South Africa, Pretoria.

Kalusopa, T & Zulu, S. 2009. Digital heritage material preservation in Botswana: problems and prospects. *Collection Building* 28(3):98-107.

Kamatula, GA. 2010. E-government and e-records: challenges and prospects for African records managers and archivists. *ESARBICA Journal* 29:147-164.

Kamatula, GA. 2012. The legal and regulatory framework and infrastructures for e-government initiatives in Tanzania: a critical review. *Mousaion* 30(2):41-55.

Kanyengo, CW. 2006. Managing digital information resources in Africa: Preserving the integrity of scholarship. Paper presented at the Bridging the North-South Divide in Scholarly Communication on Africa, Leiden, September.

Katuu, S & Ngoepe, M. 2015. Managing digital records in a South African public sector institution, in Anderson, K, Duranti, L, Jaworski, R, Stanic, H, Seljan, S & Matljan, V (eds), *INFuture2015 e-institutions-openness, accessibility and preservation.* Crotia: University of Zagreb.

Keakopa, SM. 2007. The management of electronic records in Botswana, Namibia and South Africa: opportunities and challenges. D Phil thesis, University College London, London.

Keakopa, SM. 2008. Trends in long-term preservation of digital information: challenges and possible solutions for Africa. Paper presented at the Conference on Electronic Publishing and Dissemination, Dakar, October.

Keakopa, S. 2010. The trends in long-term preservation of digital information: challenges and possible solutions for Africa. *Africa Media Review* 18(1&2):73-84.

Kemoni, HN. 2007. Records management practices and public service delivery in Kenya. D Phil thesis, University of KwaZulu-Natal, Pietermaritzburg.

Kemoni, H & Ngulube, P. 2008. Relationship between records management, public service delivery and the attainment of the United Nations millennium development goals in Kenya. *Information Development* 24(4):296-306.

Kim, YS. 2015. The importance of literature review in research writing. Available at: http://owlcation.com/misc/literature_review (Accessed 05 June 2017).

Knight, G. 2004. Report on preservation standards: SHERPA project document. Available at: http://sherpa.ac.uk/documents/D4-5_report_on_preservation_standards.pdf (Accessed 28 January 2016).

Kothari, C. 2004. *Research methodology: methods and techniques.* New Delhi: Sage Publications.

Kumar, JC. 2008. *Research methodology.* New Delhi, SB: Nangia.

Laudon, KC & Laudon, JP. 2005. *Essentials of management information system: managing the digital firm.* 6th edition. New Jersey: Pearson Education.

Leedy, P & Ormrod, J. 2005. *Practical research: planning and design.* 7th edition. Upper Saddle River, NJ: Pearson.

Lemieux, VL. 2016. *One step forward, two steps backward? Does e-government make governments in developing countries more transparent and accountable.* Washington (DC): World Bank.

Lester, FK. 2005. The theoretical frameworks, conceptual and philosophical foundations for research in mathematics education. *ZMD: International Reviews on Mathematical Education* 37(6):457-460.

Linux Information Project. 2005. Checksum definition. Available at: http://www.linfo.org/checksum.html (Accessed 05 September 2016).

Liu, BOS. 2013. Digital preservation strategies at Colarado State University libraries. *Library Management* 34(1):83-95.

Lor, P. 2005. Preserving African digital resources: is there a role for repository libraries? *Library Management* 26(12):63-72.

Lowry, J. 2012. Management and preservation of digital records in Tanzania. Available at: http://www.pokarhmb.si/uploaded/datoteke/Radenci2012/45_Lowry_2012.pdf (Accessed 30 July 2015).

Lowry, J & Nduna, V. 2015. Digital records management and preservation. Paper presented at the XXIII ESARBICA General Conference, Victoria Falls, 8-12 June.

Lupane State University. 2017. Lupane state university ICT policy. https://www.lsu.ac.zw/pdf/ICT_policy.pdf (Accessed 31 August 2017).

Luyombya, D & Obbo, DF. 2013. The state of digitisation of the land registry operations in Uganda. *Journal of the South African Society of Archivists* 46:24-35.

Maboreke, D. 2007. An evaluation of the effectiveness of records surveys in the management of public records in Masvingo Province. M Inf Dissertation, National University of Science and Technology, Bulawayo.

Mackenzie, N & Knipe, S. 2006. Research dilemmas: paradigms, methods and methodology. *Issues in Educational Research* 16:193-205.

MacNealy, MS. 1999. *Strategies for empirical research in writing.* New York: Longman.

Maki-Turja, J, Anderson, J & Huselius, J. 2016. Designing case studies. Available at: http://www.idt.mdh.se/phd/courses/fallstudie/slides%2520%2520seminarie%25202/Yin%25 20-%2520DesigningCaseStudies%2520chapter%25202.ppt (Accessed 25 October 2016).

Malemelo, F., Dube, A., David, R & Ngulube, P. 2013. Management of financial records at the Marondera Municipality in Zimbabwe. *Journal of the South African Society of Archivists* 46:12-23.

Mambo, E. 2012. Zimbabwe to go digital by 2015. *Chronicle Newspaper.* 03 January.

Manojlovich, S & Bennett, MJ. 2011. Digital preservation best practices: lessons learned from across the pond. *UConn libraries presentations.* Paper 29. Available at: http://digitalcommons.uconn.edu/libr_pres/29 (Accessed 10 September 2016).

Manyambula, MT. 2009. Public service reform, accountability and records management: A case study of Tanzania. *ESARBICA Journal* 28(2):2-33.

Marshall, C & Rossman, GB. 1999. *Designing qualitative research.* 3rd edition. London: Sage.

Marshall, C & Rossman, G. 2006. *Designing qualitative research.* 4th edition. California: SAGE Publications, Inc.

Mason, J. 2002. *Qualitative researching.* 2nd edition. London: Sage.

Mason, S. 2007. Authentic digital records: laying the foundation for evidence. *Information Management Journal* 5:32-40

Masuku, M & Makwanise, N. 2012. Archives, accountability, human rights and good governance: where is the nexus? *Mousaion* 30(2):169-181.

Matangira, V. 2016. Records and archives management in post colonial Zimbabwe's public sector. D Phil thesis, University of Namibia, Windhoek.

Mazikana, P. 2009. A missed opportunity: archival institutions and public sector reforms. *ESARBICA Journal* 28:36-51.

Miles, MB & Huberman, AM. 1994. *Qualitative data analysis.* 2nd edition. California: Sage.

Milton, MR. 2000. Electronic records and the law: causing the federal records programme to implode. D Phil dissertation, Virginia Polytechnic Institute and State University, Blacksburg.

Minnesota History Society. 2012. Electronic records management guidelines: Digital media storage. Available at: www.mnhs.org/preserve/records/electronicrecords/erstorage.php (Accessed 02 March 2017).

Mnjama, N & Wamukoya, J. 2006. E-government and records management: an assessment tool for e-records readiness in government. *The Electronic Library* 25(3):274-284.

Moatlhodi, TM. 2014. An assessment of e-records readiness at the ministry of labour and home affairs headquarters in Botswana. MARM dissertation, University of Botswana, Gaborone.

Motupu, K. 2015. Assimilation of e-government systems at the ministry of trade and industry in Botswana. MARM dissertation, University of Botswana, Gaborone.

Murambiwa, IM. 2012. Archiving to the last archivist standing: the National Archives of Zimbabwe under sanctions. *COMMA* 1:59-66.

Mutsagondo, S. 2017. Electronic records management in public departments in the Midlands Province of Zimbabwe. M Inf dissertation, University of South Africa, Pretoria.

Mutsagondo, S & Chaterera, F. 2014.Mirroring the National Archives of Zimbabwe Act in the context of electronic records: lessons for ESARBICA member states. *Information Development*. Available at: http//idv.sagepub.com/content/early/2014/06/16/026666691453872 (Accessed 05 November 2015)

Mutsagondo, S & Tsvuura, G. 2015. Dilemma in the disposition of e-mail records in public departments in Zimbabwe: the case of the Midlands Province. Paper presented at the XXIII ESARBICA General Conference, Victoria Falls, 8-12 June.

Mwangi, PW & Wamukoya, JM. 2012. Digital preservation of agricultural information at Kenya Agricultural Institute. *ESARBICA Journal* 31: 99-110.

Nachimias, C & Nachimias, D. 1996. *Research methods in the social sciences.* 5th edition. London: St Martin's Press.

National Archives of Australia, 2017. Storing digital information. Available at: www.naa.gov.au/information-management/managing-information-and-records/storing/storing-digital/index.aspx (Accessed 02 March 2017).

National Archives and Records Administration (NARA). 2013. White paper on best practices for the capture of social media records. Available at: http://www.archives.gov/record-mgmt/resources/socialmediacapture.pdf (Accessed 19 August 2016).

National Archives and Records Service of South Africa. 2006. *Managing electronic records in governmental bodies: policy, principles and requirements*. Pretoria: NARS.

National Archives of Southern Rhodesia. 1969. *Guide to the public archives of Rhodesia*. vol 1. 1890-1923. Salisbury: National Archives of Southern Rhodesia.

National Archives of St Kitts and Nevis. 2011. Access policy. Available at: http://www.nationalarchives.gov.kn/index.php (Accessed 17 March 2017).

National Archives of Sweden. 2005. Digital preservation in Archives: Overview of current research and practices. Available at: http//www/ltu.se/cms_fs/1.83844:/file/Digital%20Preservation%20in%20Archives.pdf (Accessed 10 June 2015).

National Archives of UK. 2011. Digital preservation policies: guidance for archives. Available at: http://www.nationalarchives.gov.uk/documents/information-management/digital-preservation-policies-guidance-draft-v4.2.pdf (Accessed 10 September 2016).

National Archives of UK .2014. The technical registry PRONOM. Available at: http://www.nationalarchives.gov.uk/PRONOM (Accessed 09 September 2016).

National Archives of Zimbabwe. n.d. *Masvingo.*

National Electronic Commerce Coordinating Council (NECCC). 2004. Challenges in managing records in the 21st century. Available at: http://library.osu.edu/assets/Uploads/RecordsManagement/Challenges-in-21st-e-recsneccc.pdf (Accessed 27 August 2015).

Ndayisaba, J. 2012. Burundi archives: policy and legislative framework, Paper presented at the international conference on African digital libraries and archives. Available at: http://hdl.handle.net/10539/11526 (Accessed 30 July 2015).

Nduna, V & Chigodora, T. 2015. More connected, more extended, more content, more risk? Mobile device explosion and its implications to the public sector records management in Zimbabwe. Paper presented at the XXIII ESARBICA General Conference, Victoria Falls, 8-12 June.

Nengomasha, CT. 2009. A study of electronic records management in the Namibian public service in the context of e-government. D Phil thesis, University of Namibia, Windhoek.

Nengomasha, CT. 2013. The past, present and future of records and archives management in sub-Saharan Africa. *Journal of the South African Society of Archivists* 46: 2-11.

Neuman, WL. 2000. *Social research methods: Qualitative and quantitative approaches,* 4th edition. Boston: Pearson Education.

Neuman, WL. 2003. *Social research methods: Qualitative and quantitative approaches,* 5th edition. New York: Oxford University Press.

Neuman, WL. 2011. *Social research methods: Qualitative and quantitative approaches,* 7th edition. Boston: Allyn & Bacon.

Ngoepe, MS. 2008. An exploration of records management trends in the South African public sector: A case study of the department of provincial and local government. M lnf dissertation, University of South Africa, Pretoria.

Ngoepe, M. 2015. When rain clouds gather – entrustment of government records to the cloud in South Africa. Paper presented at the XXIII ESARBICA General Conference, Victoria Falls, June.

Ngoepe, M. 2017. Archival orthodoxy of post-custodial realities for digital records in South Africa. *Archives and Manuscripts.* DOI: 10.1080/01576895.2016.1277361:1-14

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.

Ngoepe, M. & Van der Walt, T. 2009. Strategies for the preservation of electronic records in South Africa: Implications on access to information. *Innovation* 38:1-27.

Ngoepe, M, Mokoena, L & Ngulube P. 2010. Security, privacy and ethics in electronic records management in the South African public sector. *ESARBICA Journal* 29:36-66.

Ngoepe, M & Keakopa, SM. 2011. An assessment of the state of national archival and records systems in the ESARBICA region: A South Africa-Botswana comparison. *Records Management Journal* 21(2):145-160.

Ngulube, P. 2003. Preservation and access to public records and archives in South Africa. D Phil thesis, University of Natal, Pietermaritzburg.

Ngulube, P. 2005. Environmental monitoring and control at national archives and libraries in Eastern and Southern Africa. *Libri* 55(2-3):154-168.

Ngulube, P & Tafor, VF. 2006. The management of public records and archives in the member countries of ESARBICA. *Journal of the Society of Archivists* 27(1):57-83.

Ngulube, P. 2009. *Preservation and access to public records in South Africa.* Saarbrucken: Lambert Academic Publishing AG & Co. KG.

Ngulube, P. 2010. Mapping mixed methods research in library and information science journals in sub-Saharan Africa 2004-2008. *The International Information and Library Review* 42(4):252-261.

Ngulube, P. 2012. "Ghosts in our machines": preserving public digital information for the sustenance of electronic government in sub Sahara Africa. *Mousaion 30*(2):112-120.

Ngulube, P. 2015. Trends in research methodological procedures used in knowledge management studies (2009 – 2013). *African Journal of Library, Archives and Information Science* 24(2) (forthcoming).

Nkala, GS, Ngulube, P & Mangena SB. 2012. E-records readiness at the National Archives of Zimbabwe. Available at: http://uir.unisa.ac.za/bitstream/handle/10500/18284/PatGuguMangena.pdf?sequence=1 (Accessed 13 May 2015).

North Carolina Department of Cultural Resource (NCDCR). 2012. Best practices for state agency social media usage in North Carolina version 2.0. Available at: http://digitalpreservation.ncdcr.gov/best_practices_socialmedia_stateagency.pdf (Accessed 02 September 2016).

Oates, B. 2006. *Researching information systems and computing.* London: Sage.

Ohio Electronic Records Committee. 2012. Social media: the records management challenge. Available at: http//ohsweb.ohiohistory.org/ohioerc/images/c/c6/OhioERC-Guideline-social-media.pdf (Accessed 19 August 2016).

Olsen, W. 2012. *Data collection: key debates and methods in social research.* London: Sage.

Parahoo, K. 1997. *Nursing research: principles, process and issues.* London: Macmillan Press.

Parer, D. 2000. Archival legislation for commonwealth countries. Available at: http://www.acarm.org/oid%255C1_1_3_41_05_PM_Legislation%252Report.pdf (Accessed 01 June 2017)

Patton, M. 1990. *Qualitative evaluation and research methods.* 2nd edition. Newbury Park: Sage.

Patton, MQ. 2002. *Qualitative research and evaluation methods.* 3rd edition. London: Sage.

Patton, MQ & Cochran, M. 2002. A guide to using qualitative research methodology. Available at: http://www.alnap.org/pool/files/qualitative-research-methodology.pdf (Accessed 10 October 2016).

Perry, DE. 2000. Case Studies. Available at: http://users.ece.utexas.edu/~perry/education/382c/L06.pdf (Accessed 25 October 2016).

Perry, SR. 2014. Digitisation and digital preservation: A review of the literature. *SLIS Student Research Journal* 4(1):1-12.

Punch, KF.1998. *Introduction to social research: quantitative and qualitative approaches*. New Delhi: Sage Publications.

Redfern, S & Norman, I. 1994. Validity through triangulation. *Nurse research* 2(2):41-56.

Rinehart, AK, Prud'homme, PA & Hout, AR. 2014. Overwhelmed to action: digital preservation challenges at the under resourced institution. *OCLC Systems and Services* 30(1):28-42.

Rogers, C & Duranti, L. 2012. Educating records professionals on topics in digital preservation. Available at: www.ica-sae.org/Education%20Modules.pdf (Accessed 10 June 2015).

Ruhonde, E, Owei, V & Maumbe, BM. 2008. Arguing for the enhancement of public service efficiency and effectiveness through e-government: the case of Zimbabwe. Available at: http://www.gisp.gov.zw/index.php/downloads/category/10egovernment?download=15:unpan031154 (Accessed 6 August 2015).

Samuelsson, G, Oberg, LM & Borglund, E. 2007. Long term preservation of complex and integrated e-services. Available at: https://www.mium.se/siteassets/forskning/centre-och-institut/cedif/bygga-villa/56-e-services-and-long-term-preservation-last-version.pdf (Accessed 28 August 2016).

Sanett, S. 2013. Archival digital preservation programs: staffing, costs and policy. *Preservation Digital Technology and Culture* 42(3):137-149.

San Francisco Edit, 2017. Fourteen steps to writing an effective discussion section. Available at: http://cancer.dartmouth.edu/documents/pdf/effective_discussions.pdf (Accessed 12 July 2017).

Sauro, J. 2015. Five types of qualitative methods. Available at: http://measuringu.com/qual-methods/ (Accessed 16 June 2017).

Schram, TM. 2003. *Conceptualising qualitative inquiry.* New Jersey: Merrill Prentice Hall.

Schwandt, TA. 2007. *The sage dictionary of qualitative inquiry.* Thousand Oaks, CA: Sage.

Shenton, AK. 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information* 22:63-75.

Shinder, D. 2006. Ten things you can do to protect your data. Available at: www.techrepublic.com/article/10-things-you-can-do-to-protect-your-data/ (Accessed 02 March 2017).

Silverman, D. 2001. *Interpreting qualitative data: methods for analysing talk, text and interaction.* 2nd edition. London: Sage.

Smith, K. 2007. *Public sector records management: a practical guide.* Burlington: Ashgate Publishing Limited.

Sugimoto, S. 2008. Ensuring the preservation and use of electronic records, in *The 8th General Conference of EASTICA and Seminar: Development of the government and digital records management, Tokyo, Japan, October 2007. Proceedings,* edited by EASTICA: 56-67. Available at: http://www.eastica.org/EAArchive/EAA14/EAA14.pdf (Accessed 26 August 2015).

Sugimoto, S. 2014. Digital archives and metadata as critical infrastructure to keep community memory safe for the future – lessons from Japanese activities. *Archives and Manuscripts* 42(1):61-72.

State Archives of North Carolina. 2012. File format guidelines for management and long-term retention of electronic records. Available at: http://digitalpreservation.ncdcr.gov/ (Accessed 20 April 2017).

Surbhi, S. 2016. Difference between probability and non-probability sampling. Available at: Keydifferences.com/difference-between-probability-and-non-probability-sampling.html (Accessed 20 July 2016).

Tashakkori, A & Teddlie, C. 2003. Major issues and controversies in the use of mixed methods in social and behavioural sciences, in Tashakkori, A & Teddlie, C (eds), *Mixed Methods in Social and Behavioural Research.* Thousand Oaks, CA: Sage.

Tashakkori, A & Teddlie, C. 2010. Preface, in Tashakkori, A & Teddlie, C (eds), *SAGE handbook of mixed methods in social and behavioural research.* 2nd edition. Thousand Oaks, CA: Sage: ix-xv.

Tasmanian Archive Heritage Office (TAHO). 2015. State records guideline number 19: digital preservation formats. Available at:

https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%2520Library%2520%2520%Tools/Guideline%252019%2520%Digital%2520Preservation%2520formats.pdf (Accessed 30 August 2016).

Thanye, KG. 2014. An assessment of appraisal practices of architectural records at the Gaborone City Council in Botswana. MARM dissertation, University of Botswana, Gaborone.

Thibodeau, K. 2014. Missing links: What happens to the chains of custody and preservation in the cloud? Available at: https://interparestrust.org/assets/public/dissemination/ThibodeauSAA20140814.pdf (Accessed 17 July 2015).

Thomas, S. 2006. Selecting the right preservation strategy. Available at: http://www.paradigm.ac.uk/wookbook/preservation-strategies/selecting-other.html (Accessed 18 August 2016).

Thurston, A. 2012. Trustworthy records and open data. *The Journal of Community Informatics* 8(2). Available at: http://ci-journal.net/index.php/ciej/article/view/951> (Accessed 23 October 2017).

Tiwari, S. 2013. Chapter-4: Presentation, analysis and interpretation of data. Available at: http://shodhganga.inflibnet.ac.in/bitstream/10603/16098/10/11_chapter%25204.pdf (Accessed 28 June 2017).

Trochim, B. 1999. Research methods: field research and types of observation. Available at: http://www.staff.city.ac.uk/j.s.labonte/pdf/fieldandobservationresearch.pdf (Accessed 13 June 2015).

Trochim, WMK. 2006. *Research methods knowledge base.* New York, NY: Concept Systems Knowledge Base.

Tsvuura, G & Mutsagondo, S. 2015. The role of tertiary education institutions in the development of the records and management discipline in Zimbabwe. *International Journal of English and Education 4*(2):458-470.

United Nations. 2010. *United Nations e-government survey 2010: leveraging e-government at a time of financial and economic crisis.* New York: United Nations.

United Nations. 2014. United nations e-government survey 2014: e-government for the future we want. Available at: (Accessed 18 September 2016).

Urquhart, C. 2015. Observation research techniques. *Journal of EAHIL* 11(3):29-31.

Vosloo, JJ. 2014. Chapter 6: Data analysis and presentation. Available at: http://dspace.nwu.ac.za/bitsream/handle/10394/12269/Vosloo_JJ_chapter_6.pdf (Accessed 29 June 2017).

Voutssas, J. 2012. Long-term digital information preservation: challenges in Latin America. *Aslib Proceedings* 64(1):83-96.

Wamukoya, J & Lowry, J. 2013. A regulatory framework for the management of records: assessments in Kenya, Uganda and Tanzania. *ESARBICA Journal* 32:151-159.

Wamukoya, J & Mutula, SM. 2005. E-records management and governance in East and Southern Africa. *Malaysian Journal of Library and Information Science* 10(2):67-83.

Wanjohi, AM. 2012. Importance of literature review. Available at: http://www.kenpro.org/importance-of-literature-review/ (Accessed 05 June 2017).

Welman, C., Kruger, F & Mitchell, B. 2005. *Research methodology.* 3rd edition. Cape Town: Oxford University Press.

World Bank & IRMT. 2000. Managing records as a basis for effective service delivery and public accountability in development: an introduction to core principles for staff of the World Bank and its partners. Available at: http://siteresources.worldbank.org/EXTARCHIVES/Resources/Core%20Principles.pdf (Accessed 28 July 2016).

Wright. J. 2014. Paper vs electronic: The not-so-final-battle. Available at: https://siarchives.si.edu.blog/paper-vs-electronic-not-so-final-battle (Accessed 27 March 2017).

Yin, R. 1994. *Case study research: design and methods*. 2nd edition. Beverly Hills: Sage.

Yin, RK. 2003. *Case study research: design and methods*. 3rd edition. London: Sage.

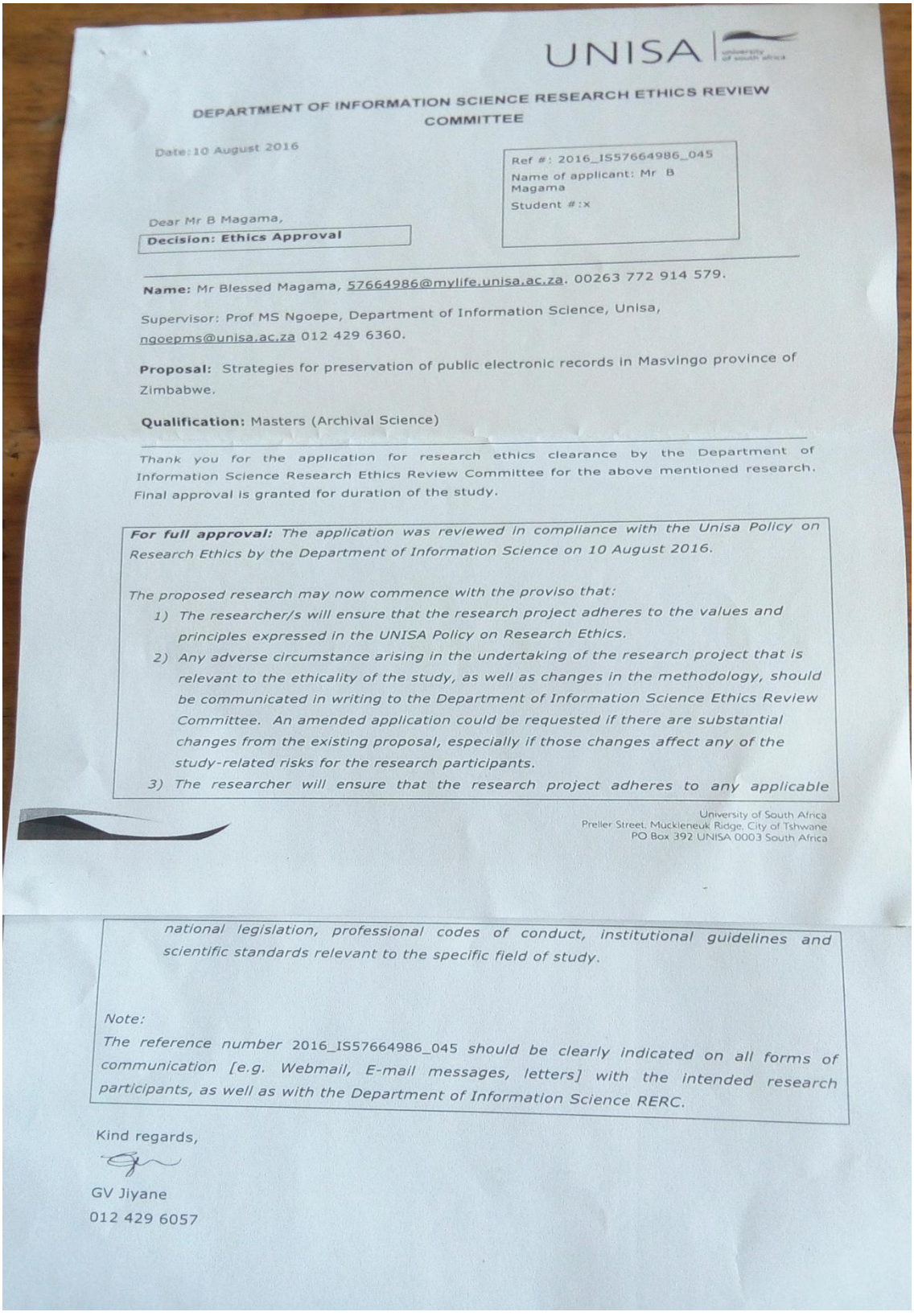
Yin, RK. 2009. *Case study research: design and methods*. 4th edition. California: Sage.

Zeblith, F, Fernandez, M & Rowe, M. 2012. Production and consumption of university linked data. *Interactive Learning Environments* 5:15-25

Zimbabwe. 1986. *National Archives of Zimbabwe Act Chapter 25:06 no.8 of 1986.* Harare: Government Printers.

Zimbabwe. 2003. Access *to Information and Protection of Privacy Act (AIPPA) Chapter 10:27 of 2003*. Harare: Government Printers.

Appendix A: Ethical clearance from UNISA



UNISA

DEPARTMENT OF INFORMATION SCIENCE RESEARCH ETHICS REVIEW COMMITTEE

Date: 10 August 2016

Ref #: 2016_IS57664986_045
Name of applicant: Mr B Magama
Student #:x

Dear Mr B Magama,

Decision: Ethics Approval

Name: Mr Blessed Magama, 57664986@mylife.unisa.ac.za. 00263 772 914 579.

Supervisor: Prof MS Ngoepe, Department of Information Science, Unisa, ngoepms@unisa.ac.za 012 429 6360.

Proposal: Strategies for preservation of public electronic records in Masvingo province of Zimbabwe.

Qualification: Masters (Archival Science)

Thank you for the application for research ethics clearance by the Department of Information Science Research Ethics Review Committee for the above mentioned research. Final approval is granted for duration of the study.

For full approval: *The application was reviewed in compliance with the Unisa Policy on Research Ethics by the Department of Information Science on 10 August 2016.*

The proposed research may now commence with the proviso that:

1) *The researcher/s will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.*
2) *Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Department of Information Science Ethics Review Committee. An amended application could be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants.*
3) *The researcher will ensure that the research project adheres to any applicable*

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa

national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study.

Note:
The reference number 2016_IS57664986_045 should be clearly indicated on all forms of communication [e.g. Webmail, E-mail messages, letters] with the intended research participants, as well as with the Department of Information Science RERC.

Kind regards,

GV Jiyane
012 429 6057

Appendix B: Letter for seeking authority to conduct research in departments

05 December 2016

The Head
Ministry/ Department of……..
Masvingo

Dear sir/madam

RE: Request for Permission to Conduct Research in Your Organisation

My name is Blessed Magama and I am doing research with Mpho Ngoepe, a Professor in the Department of Information Science who is my supervisor towards a Master of Information Science in Archival Science degree at the University of South Africa.

I am conducting research on strategies for preservation of digital records in Masvingo province of Zimbabwe. The aim of the study is to examine the current strategies for preservation of digital records in Masvingo province with a view to make recommendations for effective preservation of public sector digital records to guarantee their continued accessibility. All research data will be solely used for academic purposes. The research will involve interviewing records management officer, information technology (IT) officer and one administration officer preferably the head of department at provincial level. It will also include making observations of digital preservation activities and facilities and review of digital preservation supporting documents. I therefore seek authorisation to carry out interviews, make observations and consult relevant digital preservation supporting documents at your office. Once permission is granted, I will make appointments with the relevant officers for data collection sessions.

I look forward to your consideration of my request.

Yours sincerely,

Blessed Magama
Cell: 0772 915 579 Email: 57664986@mylife.unisa.ac.za or magamablessed6@gmail.com

Appendix C: One of the permission letters to conduct research in departments

RURAL ELECTRIFICATION AGENCY

MASVINGO PROVINCE
1st Floor Zimre Building
Cnr Hughes St/Simon Mazorodze Mvo
P.O Box 487 Masvingo
Tel: 039 262583/262527
Fax: 039 264011
Email: rea-masvingo@rea.co.zw

OUR REF: NC/hr/af
YOUR REF:.....
WHEN CALLING WITH REFERENCE
TO THIS LETTER PLEASE ASK FOR
Mr Chida

09 January 2017

Blessed Magama
National Archives of Zimbabwe
Masvingo Records Centre
4th Floor ZIMRE Building
MASVINGO

Dear Sir

REF: REQUEST FOR PERMISSION TO CONDUCT A RESEARCH

Reference is made to your application dated 05 December 2016 on the above subject.

Please be advised that the request for you to conduct a research with the Agency on Strategies for Preservation of Electronic (digital) Records in Masvingo Province is accepted. You are however requested to note that the information provided should only be used for your academic research paper and not for anything else.

Yours faithfully

Eng. E. Masendu
PROVINCIAL RURAL ELECTRIFICATION MANAGER - Masvingo

Board Members: W. Chiwewe (Chairman); C. Chitiyo (Vice Chairman); M. Khumalo; F. Chikovo; J.T. Jaji; F.S. Mbetsa; C. Shumba; C. Moyo; J.V. Mashamba (CEO)

Appendix D: Respondent consent form

I ……. confirms that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

He explained to me and I understood the nature of the research. I have had sufficient opportunity to ask questions and I am prepared to participate in the study. I understand that my participation is voluntary and that I am free to withdraw at any time without penalty. I am aware that the findings of this study will be processed into a research report, journal publications and conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree or do not agree to the recording of the interview (Delete inapplicable).

Participant Name and Surname:……..
Participant Signature:……..
Date:……..

Researcher's Name and Surname:…….
Researcher's Signature……..
Date:……..

Appendix E: Interview guide

Name of respondent:

Department:

Website address:

Gender

Designation:

Number of years in the current position:

Date of interview:

SECTION A: DIGITAL RECORDS PRESERVATION

1. When did you start generating and preserving digital records at this department?

2. Can you give me the types of digital records preserved at this department?

3. Who is charged with the preservation of these records?

4. How do you select records for preservation into your archival custody?

5. Who is responsible for selecting digital records for preservation?

6. In which standard format(s) do you preserve your digital records?

7. How do you store the digital records ingested into your archival custody?

8. Briefly explain the digital preservation strategy or strategies you use at this department?

9. What social media platforms does your organisation use?

10. What does it use it for?

11. How do you preserve records generated through social media platforms?

12. If you are not preserving records generated through social media platforms, what could be the reasons?

SECTION B: LEGAL, STANDARDS AND POLICY GUIDELINES

13. What policies or legislative frameworks guide you in the preservation of digital records?

14. To what extent do the policies or legislative frameworks meet your organisation's current digital preservation needs?

15. How does your department manage issues of compliance to the policies or legislative frameworks?

16. Which standards does your organisation benchmark against its digital preservation?

SECTION C: ACCESS, SECURITY AND PRIVACY ISSUES

17. Who have access to the preserved digital records at your department?

18. How do you provide access to the preserved digital records?

19. How do you ensure that digital information preserved remains accessible in future?

20. What security and privacy challenges does your institution experience with respect to the preserved digital records?

21. How do you protect the preserved records from unauthorised access?

22. How do you protect the preserved records from tempering?

23. How do you protect the preserved records from viruses and malicious softwares?

24. What plan(s) are in place to salvage your digital records in the event a disaster strikes?

SECTION D: RESOURCES FACILITIES AND TOOLS

25. What resources, facilities and tools are available for preservation of digital records?

26. How large is your digital repository e.g. in GB or TB

27. Do you have an annual budget for digital preservation activities? Give details.

SECTION E: TRAINING AND STAFFING

28. Who is responsible for digital preservation at this organisation?

29. Who is responsible for maintenance of your digital repository at this organisation?

30. What other responsibilities do these people have?

31. What qualifications do they possess?

SECTION F: RECOMMENDATIONS AND SUGGESTIONS

32. What are the problems that you see regarding the general preservation of digital records? [Probe: Reasons for these problems if any.]

33. How can the digital preservation function at your department strengthened?

34. What future plans does your department have with respect to the preservation of digital records?

35. Any suggestions?

Thank you for your time and contribution

Appendix F: Observation checklist

In the process of observing digital preservation practices and systems, the researcher will pay special focus on the following:

- Digital preservation strategies and procedures.
- ICT equipment.
- Personnel involved in digital preservation processes.
- Digital records preservation systems.
- Types and classes of records preserved.
- Digital preservation environment.

Appendix G: List of documents analysed

The researcher reviewed the following documents from the departments under study:

- Preservation policy or guidelines.
- Retention and disposal policy or guidelines.
- Guidelines for handling storage media
- Repository audit checklist.
- ICT policy.
- Access policy
- Disaster management plans

Appendix H: National Archives of Zimbabwe: Records survey worksheet

MINISTRY/DEPT……..

Date established…….

Headed by……

Designation ……

Staff compliment ……

Registry staff ……

Training in Records Management……

1)FUNCTIONS……
……
……

2)

Records Classes	**Covering Dates**	**Quantity**

3) FILING CONTROL SYSTEMS e.g. alphabetical, numeric, etc
……
……
……

4) FILING EQUIPMENT (Type and Size)
……
……
……..

5) RETENTION AND DISPOSAL POLICY
……
……

6) STORAGE

i)Do you store semi current records in your office?
……

ii) When do you transfer Records to your store rooms/ strong rooms?
……

iii) Do you utilize Records Centre Services?
……
……

iv) Records Centre Operations Awareness

……..

v) Date of last deposit

……

7) DO YOU STORE VITAL RECORDS (Information absolutely essential to the functioning survival and reconstruction of the organization)

……

……

8) DO YOU HAVE A VITAL RECORDS MANAGEMENT PROGRAMME

……

……

9) ACCESS TO REGISTRY (Unauthorized entry etc)

……

10) SECURITY PRECAUTIONS OF RECORDS AGAINST

a) Fire……

b) Pests……

c) Sunlight……

d) Dust……

e) Water……

11) DO YOU GENERATE AND STORE E- RECORDS

……

……

12) PROBLEMS / OBSERVATIONS

……

……

……

……

……

……

……

……

……

……

……

……

……

……

Survey conducted by……Date……..

Appendix I: List of public departments targeted to participate in this study

Name of department	Physical address in Masvingo city
Zimbabwe Tourism Authority (ZTA)	2nd Floor ZIMRE Building
National AIDS Council (NAC)	Number 5 Greenfiel Street
Masvingo General Hospital	75 Hay Robertson Road Rhodene
Veterinary Services	Herbert Chitepo Street
Masvingo City Council	Civic Centre Gardens
Zimbabwe Revenue Authority (ZIMRA)	3rd Floor ZIMRE Building
Registrar General	Number 13 & 14 Simon Mazorodze Street
Zimbabwe Open University (ZOU)	68 Hellet Street
National Museums and Monuments	Great Zimbabwe Monuments site
Information and Publicity	Ground floor Benjamin Burombo House
Rural Electrification Agency	1st Floor ZIMRE Building
Forestry Commission	2850 Chibuku Drive
Agricultural Technical Extension services	2nd Floor Benjamin Burombo House
National Social Security Authority	Compensation House Building, Robertson Street
Premier Service Medical Aid Society	Number 44 Robertson Street