DIGITAL PRESERVATION MATURITY AT THE OFFICE OF THE PRIME MINISTER OF NAMIBIA

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF ARTS (RECORDS AND ARCHIVES MANAGEMENT)

OF

THE UNIVERSITY OF NAMIBIA

BY

ASSER LAUDIKA NAPANDULWE NAKALE

201201492

APRIL 2023

SUPERVISOR: PROF. TRYWELL KALUSOPA

ABSTRACT

Digital preservation involves actions that are aimed at making sure that digital records remain accessible for as long as they are needed. In order to assure the effective long-term preservation of digital records, certain standards and best practices have to be met and adhered to. Assessing the effectiveness of digital preservation is crucial, particularly for organisations that are in the business of digital preservation. This study investigated and assessed the extent to which digital preservation is carried out in the context of the Office of the Prime Minister (OPM) of Namibia. A qualitative case study was the appropriate design for the study. The population of this study consisted of individuals that were involved in the entire process of the preservation of electronic records with long-term or permanent values, specifically staff members of the EDRMS department and the OPM at large. At the time of conducting the study, the OPM had a total of three hundred and eighty-seven (387) staff members. A census sampling technique was applied to include all seven (7) members of the EDRMS Department. Using the snowball technique, the Head of Archive referred the researcher to two (2) staff members from each of the twelve (12) departments, bringing the total sample to thirty-one (31). This study made use of semi-structured interviews and observation as the data collection methods and these were supplemented by document reviews. The collected data collected were analysed through content analysis. Among others, the main findings of the study include the unavailability of a digital preservation policy and strategy, formal information governance, collaboration framework, and written agreements with users and producers. The study also found that the institution did not provide extra training to its staff members and as such, they did not have specialised and professional technical expertise.

The study recommended that the OPM should implement a Digital Preservation Policy and invest in collaboration, training and grooming of specialised professional technical expertise.

Keywords: Digital Preservation Capability Maturity Model, digital preservation, digital preservation maturity, digital preservation repository, records management, Electronic Documents and Records Management System

TABLE OF CONTENTS

DECLARATION

I, Asser L. N. Nakale, hereby declare that this is my own work and is a true reflection of my research, and that this work, or any part thereof has not been submitted for a degree at any other institution.

Asser L N Nakale		April 2023
Name of Student	Signature	Date

DEDICATION

First and foremost, I dedicate this project to the Almighty God, who has always been my source of inspiration, knowledge and understanding. Without him and his interventions throughout my life, this study would not have been possible. Secondly, I dedicate this work to my parents, Ammon Nakale and Ndilipunye Shixungileni, whose encouragement and support, both financially and psychologically, made it possible for me to complete this project. To my friend Likius Katengele, for being such an inspiration – I dedicate this one to you. You have made a brave decision of quitting a nearly completed degree course to pursue your dream career, something that is really inspirational. The commitment you have demonstrated in realising your dream is unmatched. Finally, to my brother and friend in academia, Henry Nakale, what you have achieved academically in the past five years, against all odds, is legendary. You are nothing short of an epitome of perseverance. My heartfelt love and appreciation to you all. Thank you.

ACKNOWLEDGEMENTS

I acknowledge the following people and institutions, whose efforts and guidance made this study a success. I appreciate you all.

- My supervisor, Prof. T. Kalusopa, for your patience, guidance and professionalism.
- Executive Director, OPM Mr I-Ben Nashandi, for granting me permission to carry out this study.
- Ms Helena M. Shifindi, Chief Archivist at the OPM, for helping me with scheduling interviews.
- The entire Office of the Prime Minister and individual participants.
- My family, friends and everyone that believed in me.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ISO	-	International Organisation for Standardisation
TDR	-	Trustworthy Digital Depository
DPM	-	Digital Preservation Maturity
DPCMM	-	Digital Preservation Capability Maturity Model
OPM	-	Office of the Prime Minister
EDRMS	-	Electronic Documents and Records Management System
DPM	-	Digital Preservation Maturity
OAIS	-	Open Archival Information Systems
DPC	-	Digital Preservation Capability
OS/TN	-	Open Standard Interoperable Technology Neutral Formats
AIPs	-	Archival Information Packages
PDI	-	Preservation Description Information
DIPs	-	Dissemination Information Packages
SIPs	-	Storage Information Packages
IT	-	Information Technology
PDF	-	Portable Document Format

CHAPTER ONE

BACKGROUND OF THE STUDY

1.1 Introduction

This chapter introduces and provides a background to the study. Firstly, the chapter explains the term Digital Preservation and how it has evolved over time. This is then explained within the context of Namibia, focusing mainly on the implementation of the Electronic Document and Records Management System (EDRMS) in the public sector. The chapter also presents the problem statement, research questions of the study, the relevance and the significance of the study. It finally concludes with an overview and structure of the five chapters of the study.

1.2 Orientation of the study

Digital Preservation refers to the process of making sure that digital information worthy of long-term preservation is kept in existence and remain accessible and readable for as long as it is needed (Wilson, 2017, p.130). In a technologically advanced world, records in digital forms are rapidly replacing paper records as sources of information with traceable authenticity as well as reliability (Hughes, 2014). Moreover, advanced countries started with digital preservation for some time. For underdeveloped and developing countries, digital preservation is a more recent phenomenon but it is improving rapidly on a daily basis (Bulow & Ahmon, 2011).

It has been noticed that there is a great need of assessment, as far as digital preservation programs are concerned. It is vital for institutions in the business of preserving digital records with long-term value, to assess the effectiveness and maturity of their digital preservation programs (Blumenthal et al., 2020).

Furthermore, in order to ensure the effective long-term preservation of digital records, certain standards and best practices have to be met and adhered to with regards to International Records Management standards such as ISO 14721 and ISO 16363, with respect to the reference model for an open archival information system (OAIS), as well as the audit and certification of a trustworthy digital repository (TDRs) (Dollar & Ashley, 2015).

The effectiveness of the organisation's digital preservation plays a vital role in ensuring not only the condition, but also the usability of digital records (Redweik et al., 2017). Therefore, organisations are expected to assess and know their digital preservation maturity (DPM), which is the extent to which an organisation has gone in terms of effective digital preservation (Dollar et al., 2014).

International records management standards have outlined records management best practices and guidelines on how digital information can be properly preserved, for it to remain in existence for as long as it is needed (Wilson, 2017). Although ISO 14721 and ISO 16363 specify the functions and preservation services as well as the audit and certification of Trustworthy Digital Repositories (TDRs) respectively, conducting a gap analysis of current digital preservation capabilities has remained a challenge, hence the development of the Digital Preservation Capability Maturity Model (DPCMM) (Dollar et al., 2014).

The DPCMM is used to conduct a gap analysis of current digital preservation capabilities and to help practitioners and organisations to delineate a multi-year roadmap of incremental improvements (Dollar et al., 2014).

There are three major components which influence digital preservation maturity as per the DPCMM. These components are namely, infrastructure, preservation repository and digital preservation services (Gallinger, 2021).

Infrastructure consists of all resources that are available in an institution in terms of digital preservation. The effectiveness of the institution's infrastructure would depend on the sustainability and adequacy of its resources. This involves making sure that the institution has the required level of technical expertise and competitive technologies as far as digital preservation is concerned. Digital preservation infrastructure allows the preservation repository to make appropriate digital preservation decisions (Ashenfelder, 2017).

Digital preservation repository points to the environment that ensures that all digital records that merit long-term preservation are accessible and readable for as long as they are needed. The trustworthiness of a digital repository depends on its ability to make provisions for access to authentic records for its users for as long as it is needed. In digital preservation, trustworthiness can only be achieved if there are proper policies and strategies in place (Rosa et al., 2017).

Digital preservation services include all tasks performed collectively by the staff involved in digital preservation as well as repositories, in making sure that digital records remain not only secure, but also trustworthy and usable.

It includes how the safety and security of electronic records are insured throughout all the processes and the business actions involved in digital preservation. Digital preservation services involve the efforts of all stakeholders involved in the management of electronic records (Ruusalepp & Dobreva, 2015).

It is therefore important that the evaluation and assessment of digital preservation programmes pay attention to those three major components, because collectively, they play a major role in ensuring effective digital preservation. It is important that users and producers are included in any digital preservation assessment because they are the main stakeholders in digital preservation (Gallinger, 2021). In Namibia, several institutions both in the public and private sector, have over the years acknowledged and introduced digital preservation, particularly the Office of the Prime Minister, (OPM, 2009).

Being the leader of the government business in parliament, with the mandate to coordinate the work of the cabinet as the head of administration, the present researcher believes that the OPM holds large volumes of digital records/archives, which makes it arguably one of the organisations with the biggest digital archive in the country (OPM, 2009).

The OPM has over the years introduced the Electronic Documents and Records Management System (EDRMS), with the main aim to ensure a risk-free records and archival system for the public service of Namibia (OPM, 2009). It is, however, not established how effective digital preservation is at the OPM.

It is against this background that this study assessed the extent to which the OPM has gone as far as digital preservation maturity is concerned.

1.3 Statement of the problem

Most studies in Namibia on digital preservation have put more emphasis on issues such as challenges faced with the preservation of audio-visual records (Iipinge & Mnjama, 2017), the establishment of digital programmes (Hillebrecht, 2011) and the preservation of electronic records management in general (Nengomasha, 2009).

Yet, at the OPM, the three major components of digital preservation, as per the DPCMM, have never been assessed to determine the maturity of the EDRMS. No emphasis has been put on the question and issue of current digital preservation capabilities in terms of Digital Preservation Maturity (DPM), more particularly on the assessment of DPM.

No study has ever been done to assess the EDRMS and determine its maturity in terms of digital preservation. In the absence of such a study, the effectiveness of the EDRMS and its capability to preserve and provide access to trustworthy digital records remains unknown. Therefore, currently, the OPM may have been operating the EDRMS in the absence of some very important tools of digital preservation. If it was not for this study, which investigated and assessed the extent to which digital preservation was being carried out at the OPM, shortcomings of the EDRMS would have not been identified. Equally important, the effectiveness of the EDRMS in terms of digital preservation would not be determined.

1.4 Purpose of the study

This study evaluated the digital preservation maturity of the OPM, with a focus on the EDRMS, a system which is aimed at ensuring risk-free records and archival system for the public service of Namibia (OPM, 2009).

1.5 Research objectives

The main objective of this study was to assess the Digital Preservation Maturity of the OPM.

The specific objectives were to:

1.5.1 To assess the OPM's digital infrastructure for digital preservation

1.5.2 measure the extent to which the preservation environment of the OPM adheres to the accepted operational practices as guided by standards;

1.5.3 establish the extent to which the trustworthiness of Digital Preservation Services is ensured when undertaking business actions;

1.5.4 determine the influence of producers and users on digital preservation, and

1.5.5 to give recommendations on strategies needed to be put in place for improved maturity in digital preservation.

1.6 Significance of the study

Being one of the pioneer studies of its kind in Namibia, this study is significant because:

1. It generated results and recommendations aimed at developing strategies as well as a road map for incremental capability improvement;
2. It established the importance of assessing and evaluating the effectiveness of digital preservation programmes; and
3. It contributed to the body of knowledge on digital preservation, particularly the area of Digital Preservation Maturity.

The findings of this study will be disseminated through a research report to the OPM, as the only institution that was studied, in adherence to the terms and conditions of the permission to carry out the study.

1.7 Limitations of the study

The study was qualitative; therefore, the researcher was restricted to the expressions, answers and views of the participants. These views were, however, verified through document reviews and observation as supplementary data collection methods.

In addition, some documents that the researcher thought were relevant, were deemed private and secret by the government, and as such, they could not be reviewed. For that reason, the researcher was allowed access to only a few documents.

Furthermore, this study was limited to the OPM as a case study with a purposefully selected sample and the findings can therefore not be generalised. However, the results and suggestions may be useful to all OPM departments.

1.8 Delimitations of the study

Digital preservation maturity implies the stage that the OPM's EDRMS department has attained in terms of its digital preservation programme, therefore, this study focused only on assessing the level of maturity rather than examining technical issues of digital preservation as a whole.

1.9 Definition of key terms

All key terms and phrases used throughout this study are interpreted under this section. The key terms are: digital preservation, digital preservation programme, digital preservation infrastructure, digital preservation repository, digital preservation services,

digital preservation maturity, Digital Preservation Capability Maturity Model (DPCMM), electronic records, and records management.

1.9.1 Effective Digital Preservation

Effective Digital Preservation refers to a combination of processes involved in making sure that digital information remains accessible for as long as it remains relevant (UNESCO, 2021, p.1). Even though it involves the preservation of digital materials, the effectiveness of digital preservation is determined by the ability to allow access to such material. The ultimate goal of digital preservation is to ensure access to authentic and reliable records (Massenya & Ngulube, 2019).

According to UNESCO (2021), for an institution to achieve this kind of accessibility, there are certain strategies that need to be implemented. Strategies may include:

- Working with creators and other stakeholders in identifying and implementing digital preservation good practices, to ensure the prolonged provision of access to digital records;
- Realising the importance of evaluating records and preserving only those which are worth preserving, as opposed to preserving any other information;
- Ensuring that digital materials are preserved with their full metadata, as well as protecting the integrity and authenticity of records;
- Selecting sustainable ways of providing access regardless of the changes in technology; and
- Making sure that the ultimate goal is achieved in the most cost-effective and accountable ways possible.

1.9.2 Digital Preservation Infrastructure

Digital Preservation Infrastructure may refer to the efforts of any digital preservation institution, as well as the sustainability and adequacy of its resources in ensuring effective digital preservation (Ashenfelder, 2017, p. 7).

1.9.3 Digital Preservation Repository

A digital preservation repository refers to an institution that is mandated to store and maintain digital information throughout its entire lifecycle. A digital preservation repository makes sure that digital records are preserved and can be accessed for as long as they remain relevant (Rosa et al., 2017 p. 22).

1.9.4 Digital Preservation Services

Digital preservation services include the collective efforts, actions and responsibilities of digital records staff as well as repositories in ensuring both the intellectual and technical survival of electronic records. It involves actions to ensure not only the security of records, but also their integrity, usability, trustworthiness and access, which is ensured by the preservation of metadata (Ruusalepp & Dobreva, 2015).

1.9.5 Digital Preservation Maturity

Digital preservation maturity refers to the capability of an institution to effectively preserve and make accessible relevant, authentic, trustworthy and useable digital information for as long as it is needed, as per the recognised records management standards and best practices (Maemura et al., 2017, p. 1620).

1.9.6 Digital Preservation Capability Maturity Model (DPCMM)

Digital Preservation Capability Maturity Model (DPCMM) is a model and an assessment tool that is used in evaluating organisations' capabilities to maintain and make accessible electronic records which have long-term values (Dollar & Ashley, 2015, p. 2).

1.9.7 Electronic Record

An electronic record refers to information in a digital format, which serves as evidence of any transaction or activity completed by an organisation or individual (State of Michigan, n.d. p. 3).

1.9.8 Records Management

Records management is the art of maintaining, supervising and providing access to records. It includes all activities and processes involved from the creation, receipt, maintenance, use and disposal of records (Nyampong, 2015, p. 122).

1.10 Organisation of the study

This study is divided into six (6) chapters and they are outlined as follows:

Chapter one: This chapter launches the study. It gives an overview of what the study is about. In addition, it explains the notion of digital preservation, its importance and how it evolved over the years. The chapter also presents the problem statement, as well as the research questions of the study. The relevance and significance of the study are also presented in this chapter. It concludes with the ethical considerations for the study.

Chapter two: This chapter addresses the theoretical framework, as well as the literature review. It introduces and explains the Digital Preservation Capability Maturity Model (DPCMM), which is the model that was adopted by this study as its theory.

It also explains the model's relation to the evaluation of digital preservation maturity, as well as why it has proven to be the most appropriate model for this study. This chapter, finally gives a narrative of literature on digital preservation and factors which affect the effectiveness of preserving digital information in connection to the objectives of the study.

Chapter three: In this chapter, the researcher details the methodology adopted by this study in the collection and analysis of data. Furthermore, the chapter explains and justifies the research paradigm and approach of the study. Equally important, the population of the study is also explained in this chapter. It also explains and justifies the sampling methods, data collection instruments and analysis methods used by this study.

Chapter four: This chapter presents qualitative data collected through interviews, observation and document review. In this chapter, data is organised and presented according to themes informed by the findings of the study.

Chapter five: This chapter discusses and interprets the data collected and presented in the previous chapter. It also discusses the collected information in relation to the reviewed literature.

Chapter six: Under this chapter, the research questions are answered. This is also the concluding chapter of the entire study, and it also identifies areas for further research within the same research topic.

1.11 Chapter summary

The chapter presented the background of the study, highlighting what other authors and previous researchers have written on the issue of digital preservation and exposing the importance of assessing the effectiveness of digital preservation programmes.

Furthermore, it outlined the statement of the problem, through the identification of the gap in the literature, which eventually led to this study.

Research objectives were also stated in this chapter, together with explanations as to why the study was relevant. The chapter also briefly highlighted the literature that was reviewed for this study as well as a brief introduction of the theory that guided it. It gave insight into the methodology employed by the study as well as how the researcher ensured that the study was ethical.

Finally, it gave an overview of how the study is organised by shedding light on what each chapter contains. The next chapter discusses the theoretical framework as well as the literature review.

CHAPTER TWO

THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 Introduction

This chapter presents the theoretical framework, as well as the literature review. It begins with highlighting the theory adopted by this study and explains how it is relevant to the study. It also explains the theory's relation to the evaluation of digital preservation maturity, as well as why it has proven to be the most appropriate theory for this study. It then presents the literature that informed the study.

2.2 Theoretical framework

A theoretical framework is a design plan for the whole research. Research needs to be built on a specific guide that will provide the structure to decide how the researcher will approach the whole research. A theoretical framework acts as that guide (Grant & Osanloo, 2014, p. 14). This study was guided by the Digital Preservation Capability Maturity Model (DPCMM).

The DPCMM was developed in 2011, by Charles M. Dollar and Loris J. Ashley, with the aim to provide information practitioners with an appropriate tool to plan and improve their digital preservation capabilities (Gallinger, 2021). It was created with adherence to the functions and preservation services as identified by ISO 14721, the Open Archival Information System Reference Model (OAIS) and specifications of ISO 16363, Audit and Certification of Trustworthy digital repositories (Dollar & Ashley, 2015).

Many organisations that are entitled with preserving and providing access to long-term, as well as permanent electronic records, do not have the infrastructure and resources that are adequate enough to implement a preservation repository in conformance with the ISO 14721 specifications and best practices (Dollar et al., 2014).

2.2.1 Scope of the DPCMM

The model is made up of three different but interlinked domains; Infrastructure, Digital Preservation Repository and Services. It also includes producers and users as part of the model as per ISO 14721 and 16363 Digital Preservation Standards. The model has identified fifteen (15) components as discussed in the literature review, which are regarded as important and necessary process areas in the long-term preservation and access to authentic and reliable electronic records. These components are incorporated into this model. As detailed in the literature, each of these components has its individual function, but they are related to the entire process of records preservation (Dollar & Ashley, 2015; Dollar et al., 2014; ISO, 2012; ISO, 2003).

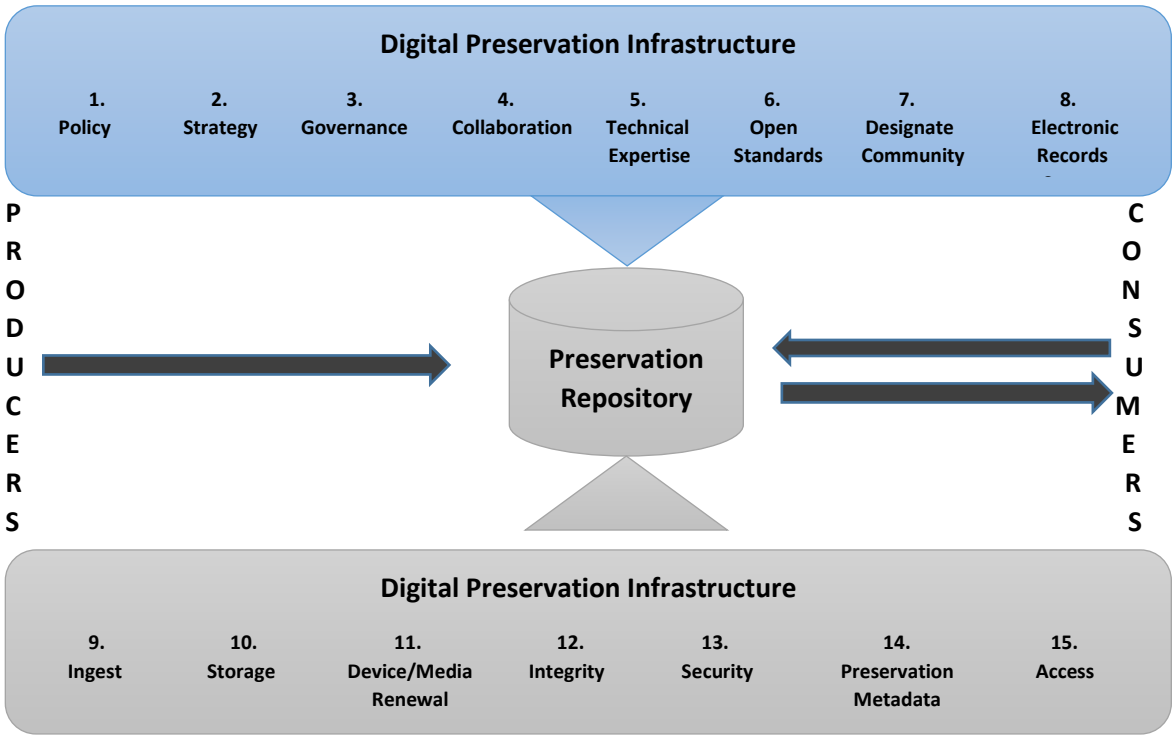


Figure 1: Scope of the DPCMM (Dollar & Ashley, 2015)

2.2.2 Digital preservation capability metrics

Each of the 15 components of the DPCMM has its associated set of five digital preservation capability metrics.

Each component is assessed and rated against the metrics, to determine its individual level as well as its conformance to ISO 14721, which is just below level two as shown in the table above. The combination of the assessments from the 15 individual components would then determine the overall stage of the organisation as per the DPCMM.

2.2.3 Five (5) stages of DPCMM

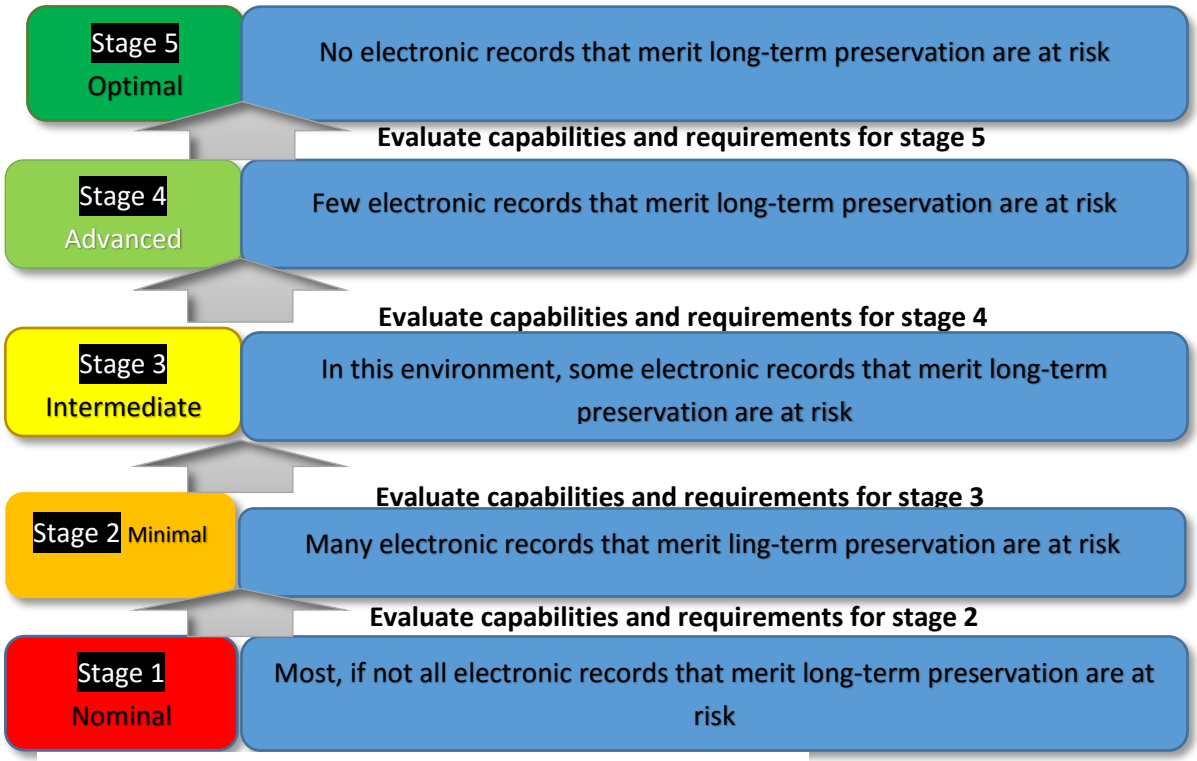


Figure 2: Five (5) Stage of the DPCMM (Dollar & Ashley, 2015)

As is the case with other capability maturity models, the DPCMM evaluates the effectiveness of digital preservation-based stages. It has five stages, with the Nominal stage being the lowest and the Optimal the highest. If an institution operates at a Digital Preservation Capability Nominal stage (Stage 1), it means that a digital preservation programme does not exist or it only exists on paper.

On the other hand, the optimal stage (stage 5), which is the highest attainable stage of Digital Preservation Capability, refers to an institution with "sustained, trustworthy capabilities that are systematically managed through process improvement and optimization" (Dollar & Ashley, 2015, p. 10).

Stage five

Being the highest level of digital preservation that an institution can achieve, stage five requires organisations to concentrate on the outcomes of digital preservation by improving the way electronic records are managed throughout their lifecycle. It also involves emulating organisations which have better digital preservation programmes and keeping on the lookout for better and advanced technologies. In this stage, only a few if any electronic records that merit long-term preservation are at risk (Dollar & Ashley, 2015).

Stage four

This stage describes an organisation with a strong infrastructure and digital preservation services, based on ISO 14721 and ISO 16363. Here, digital preservation involves collaboration of different stakeholders. Different lessons and experiences are shared amongst these stakeholders with the aim to improve digital preservation capabilities. Some electronic records that merit long-term preservation may still be at risk (Dollar & Ashley, 2015).

Stage three

Stage three describes an organisation that operates with adherence to ISO 14721 specifications and the rest of best practice standards, which normally leads to the development of advanced digital preservation capabilities over time.

This development comprises venturing into successful projects that support proper digital preservation capabilities, collaborating with other entities or sharing resources with records producers and digital repositories.

In an environment like this, many electronic records that merit long-term preservation are likely to remain at risk (Dollar & Ashley, 2015).

Stage two

Stage two describes an environment in which there is no preservation repository as per ISO 14721 specifications and requirements. In this environment, there could be a substitute preservation repository that is available and only used by some records producers, but it does not fully adhere to ISO 14721 specifications. Only a few, if any, understand digital preservation strategies. There is no link between success and failure of digital preservation initiatives, and success is mostly a result of a certain brave individual, which in most cases is not even widely shared. Most electronic records that merit long-term preservation are at risk (Dollar & Ashley, 2015).

Stage one

Stage one describes an environment in which the ISO 14721 and other electronic records management standards are not formally implemented by the department responsible for preservation or records producers. Basically, there could be a little understanding of digital preservation issues.

Some individuals in an environment like this may be attempting to store their electronic records on networks or other removable storage devices. Practically, all electronic records that merit long-term preservation are at risk (Dollar & Ashley, 2015).

2.3 Appropriateness and Relevance of the DPCMM to the study

With the main objective of the study being to assess the digital preservation of the OPM, the DPCMM proves to be the most appropriate model as it encompasses ISO standards which are important in the preservation of electronic records of long-term and permanent value, namely, the OAIS functions (ISO 14721) and Trustworthy repository audit criteria (ISO 16363). When accepted community good practices are added to those two, they set a high threshold for digital preservation capabilities (ISO, 2012; OCLC & CRL, 2007).

The five stages of the DCPMM refer to different digital preservation environments and they give descriptions of such environments. They also clearly indicate how safe those environments are for digital records which merit long-term preservation. In this case, the EDRMS is the digital preservation programme that is evaluated. The three major areas of digital preservation, namely, Digital Preservation infrastructure; Digital Preservation Services; Digital Preservation Repository; as well as the Users and Creators of information are therefore evaluated against the criteria of the DCPMM (Dollar & Ashley, 2015).

This would not only determine the effectiveness of the EDRMS programme, but it would also indicate how safe the records that are held by the EDRMS are. It would also identify areas which need improvement, as far as digital preservation is concerned. Moreover, DPCMM was made specifically for institutions and repositories with the mandate to preserve long-term and permanent electronic records to assess their capability against the ISO 14721 and ISO 16363 specifications, together with the practices accepted by the digital preservation community (ISO, 2012; ISO, 2003; OCLC & CRL, 2007).

The DPCMM was successfully used by the Council of State Archivist in July 2011 when they launched a program that aimed at improving the efforts to digital preservation as well as access to the U.S. state government electronic records nationwide. The results generated recommendations on how they can improve in terms of digital preservation and access. Funds were later made available to help effect the needed improvements (Grimm, 2016).

2.4 Literature review

Literature review is a process of critically reviewing what has already been published on the topic of interest (Milian et al., 2019, p. 134). A literature review makes it possible to determine the studies which have been conducted previously and their findings. A literature review plays a major role in assisting the researcher to identify important aspects on the topic of interest and also highlight any shortcomings of previous research. It allows the researcher to understand the topic, through existing research (Milian et al., 2019).

As far as the present research is concerned, there is no literature on digital preservation maturity, particularly in the Namibian context. However, many studies have been done in the context of other countries, most of which focussed more on digital preservation in broad terms. Some reported on the digitalisation maturity of Africa as a continent, concluding with shortcomings, challenges and recommendations (Siemens, 2017).

Some have tackled digital transformation in different industries of their countries (Ezeokoli et al., 2016), while others have researched on what is required to reach a better digital maturity level (Kane et al., 2017). In the Namibian context, most researchers in the area of digital preservation have based their studies on digital preservation in general.

Some investigated the preservation of audio-visual records (Iipinge & Mnjama, 2017) and the preservation of electronic records (Nengomasha, 2009), while others tackled the development of a digitisation programmes (Hillebrecht, 2011).

For this reason, the reviewed literature in relation to this study includes mostly online journals, articles, and documents as well as models by different authors on different aspects of Digital Preservation. This literature review is guided by the following concepts as drawn from the research objectives:

1. Sustainability and adequacy of the digital preservation infrastructure;
2. Adherence of the Preservation Repository to the accepted operational practices;
3. Safety of electronic records when undertaking digital preservation actions; and
4. The roles of producers and users in digital preservation.

These aspects are broken down further into finer subjects, for a detailed explanation and better understanding.

2.4.1 Sustainability and adequacy of the digital preservation infrastructure

Digital preservation infrastructure plays a vital role in striving to achieve the effective management of electronic records. It involves the commitment of the organisation, as well as the sustainability and adequacy of its resources in ensuring effective digital preservation (Brown, 2013). Effective digital preservation goes beyond just safely preserving digital records for as long as they are needed. It involves accession of such records and ensuring their security, which can only be achieved through adequate technical expertise and appropriate technologies (Dollar & Ashley, 2015).

Effective digital preservation requires having in place appropriate infrastructure which is crucial for the long-term continuity, access and preservation of reliable, accessible and authentic electronic records (Dollar et al., 2014).

Digital preservation infrastructure is better understood through its components and the individual roles they play in the entire process of digital preservation.

These digital preservation infrastructure components focus on what an organisation as a sole institution does in identifying records which need to be preserved. This allows the digital preservation repository to take appropriate digital preservation measures (Brown, 2013; Dollar & Ashley, 2015; Dollar et al., 2014).

These components are as follows:

1. Digital preservation policy
2. Digital preservation strategy
3. Governance
4. Collaboration
5. Technical expertise
6. Designated community
7. Electronic records survey

2.4.1.1 Digital Preservation Policy

Da Silver and Borges (2017, p. 312) define a Digital Preservation Policy as the mandate for an organisation to hold up the preservation of electronic records through an arranged and well managed digital preservation strategy.

It entails details as to why specific records need to be preserved, and it identifies how other policies related to records management should be applied to the acquisition and preservation of records. Just like there are policies which guide the management of manual records, there should be policies to guide the management of digital information. A policy makes digital preservation part of daily transaction and not just something that is done occasionally (Note, 2019).

A digital preservation policy is crucial as it explains to records creators and users how they may act to have digital records accepted for preservation (Noonan, 2014). They need to understand everything involved in digital preservation, but a policy will be needed to explain how they fit in the whole digital preservation strategy. Pinnick (2017) argues that effectively preserving accessible, authentic and reliable electronic records depends on relevant technologies, but the commitment of the organisation and its practices are equally important.

The organisation trusted with the long-term preservation of electronic records should have its policy in words. The policy should be communicated to all stakeholders and it needs to be edited occasionally for compliance. It must include the purpose, scope, accountability and approach to the transfer of records (Dollar & Ashley, 2015). Adopting a policy is vital in managing electronic records, because it sets guidelines which influence decision making (Da Silver & Borges, 2017).

Noonan (2014) highlights the lack of relevant policies as one of the worst-case scenarios in the management of electronic records. Da Silver and Borges (2017) affirm that in the business of electronic records management, operating a programme without a Digital Preservation Policy is bad practice.

According to Noonan (2014), not only does it explain why the chosen electronic records need to be preserved, but the Digital Preservation Policy also needs to pinpoint how the rest of the policies like the acquisition policy will apply to the acquisition and management of electronic records which the archive wants to preserve.

Basically, the absence of a digital preservation policy compromises some other important policies of electronic records management. This basically means that the digital preservation policy is the main policy upon which other relevant policies of electronic records management could be based (Dollar & Ashley, 2015).

Pinnick (2017) argues that there is a great need of every institution in the business of long-term preservation of electronic records, to disseminate the digital preservation policy to all its stakeholders. It is further required that the institution evaluates its conformance to the policy and reports to its governing body. The policy should also be audited and reviewed appropriately.

Da Silver and Borges (2017) agree that users and producers need to understand everything around digital preservation, therefore, they will need a policy to clearly indicate to them how they fit in the whole process of digital preservation.

This implies that in the absence of a digital preservation policy, stakeholders, including users and producers, do not have knowledge of their roles in the entire process of digital preservation. Pinnick (2017) concludes that in the absence of a Digital Preservation Policy, issues of authority and accountability are compromised.

2.4.1.2 Digital Preservation Strategy

According to Dollar and Ashley (2015, p.17), a Preservation Strategy could be defined as a set of procedures which regulate how the process of Digital Preservation will be supported. This may include: what is required of depositors before submitting their electronic records, software emulation and when it may be needed, issues of file formats, monitoring of electronic records to make sure that they remain accessible and readable, as well as the process of allowing access to records.

Digital preservation needs a strategy with proper guidance on how everything stipulated in the policy is going to be achieved. It is therefore important that a digital preservation strategy is in place (Rieager, 2018).

Expressing the significance of a strategy, Dollar and Ashley (2015) state that a digital preservation strategy is one of the most important tools in the management of electronic records. According to Shimray and Ramaiah (2018), the strategy should aim to instruct users to convert their records to "preservation ready" formats before submitting them. Also, it must call for the monitoring of any changes in technology that may affect the preservation of electronic records.

Explaining how the digital preservation strategy relates to the policy, Shimray and Ramaiah (2018) state that a Digital Preservation Strategy cannot exist in the absence of a policy. Whilst the policy gives details why the chosen electronic records need to be preserved, the strategy states how it will be implemented.

However, one strategy cannot cater for all organisations and their types of information and resources, but storage devices, media and file formats must be monitored occasionally. Failure to do so could lead to obsolete devices and media which could eventually leave bit streams of records unreadable (Shimray & Ramaiah, 2018).

2.4.1.3 Governance

An organisation that is entitled to preserve electronic records with long-term and permanent values must have a well-structured decision-making process, with relations to its information governance framework that promotes accountability and authority, digital preservation, and specifies approaches and practices for the preservation of repositories enough to satisfy the needs of stakeholders (Brooks, 2019).

Howard (2013), stipulates that in the absence of a proper governance framework, most if not all aspects of governance, inclusive of accountability and authority, are compromised. Smallwood (2013) asserts that accountability and authority are vital in identifying those that should be involved in digital preservation, both within and outside the archive and their roles. Their roles should be made clear and distinctive to ensure that they understand their authority and that they could be held accountable for their actions depending on their roles.

Equally important, in the management of records, governance framework should exist to ensure compliance of the preservation repository, with applicable laws regulations, records retention schedules, disposition authorities and standards (Dollar & Ashley, 2015). It is ideal that the organisation adopts an enterprise digital preservation governance framework, inclusive of policies and procedures, to support the repository or repositories.

Because of the possible changes in technology and other requirements, the framework must be reviewed at least after every two years (Smallwood, 2013; Dollar & Ashley, 2015).

Smallwood (2013) warns that it is a must for every organisation in the business of digital preservation to have a governance framework specifically for electronic records management. Furthermore, the governance framework should ensure compliance with all applicable laws and with adherence to both local and international standards.

This capability influences laws, practices and protocols which are already within the organisation. However, new authorities may have to be created to ensure long-term preservation and avoid technology obsolescence. Hence a preservation repository may be left with a responsibility of a technology unit. In addition, the digital preservation governance must be practiced in collaboration with information management functions and all the involved stakeholders.

The governance framework allows the repository to adhere to laws, retention schedules, disposition authorities and standards (Howard, 2013; Smallwood, 2013).

2.4.1.4 Collaboration

Altman et al. (2009) demonstrate that digital preservation involves the information structure of the organisation, the technology environment and records management standards and practices. Therefore, an organisation with a mandate to preserve electronic records with long-term as well as permanent values must maintain and promote collaboration among its stakeholders.

Pinnick (2017) claims that digital preservation involves many stakeholders, and they all play vital roles in the process, from IT, software developers and other support functions. It is thus important that the organisation's collaboration realises the relationship between and within all its stakeholders because they depend on each other.

Digital Preservation is too complex to successfully and effectively pull off as a single organisation without having to collaborate with stakeholders or other entities in the same line of business (Altman et al., 2009). It requires a lot of different resources, technologies and expertise to achieve and run an effective Digital Preservation programme (Dollar & Ashley, 2015).

Organisations in the business of digital preservation should therefore venture into collaborations with peer organisations, not only for the purpose of sharing resources, but also to share information on latest technologies and being up to date with the best systems as well as records management best practices (Pinnick, 2017). According to Dollar and Ashley (2015), a collaboration framework should not necessarily be about technical expertise, but it should see the organisation reaching out to its stakeholders to identify and eventually meet the requirements of digital preservation. Altman et al. (2009) further stipulate that many stakeholders are involved in the digital preservation and they all play vital roles in the process, from IT, software developers and other support functions. It is thus important that the organisation's collaboration realises the relationship between and within all its stakeholders because they depend on each other.

2.4.1.5 Technical expertise

For the organisation to be able to carry out the effective preservation of digital records with long-term or permanent values, it must have not only enough, but relevant expertise in electronic records management as well as digital preservation. Only then, can the organisation be able to support all of the infrastructure and processes involved in the preservation of electronic records (Pinnick, 2017).

Digital Preservation involves advanced technologies and systems which may require advanced levels of expertise in different fields and departments (Aziz et al., 2018).

It is thus highly recommended that institutions trusted with the long-term preservation of electronic records, have sufficient and qualified personnel in all positions involving electronic records management (Dollar & Ashley, 2015).

Access to technical expertise, either internally or from outside is vital throughout the entire process of digital preservation. For instance, from ingestion, users or producers must have expert assistance to help them with changing their records into preservation ready formats. This expertise would also come in handy when the repository needs to examine the potential impacts of emerging technologies on digital preservation (Dollar et al., 2014). Having qualified employees is vital, and with changes in technology, it is advisable to make sure that employees are up to date with knowledge of the latest systems, technologies and practices.

Employers should therefore organise appropriate training for their staff. Equally important, they should also have access specialised professional technical expertise, either within the organisation or externally (Pinnick, 2017).

2.4.1.6 Designated community

An organisation with a mandate to preserve electronic records effectively is required to maintain communications and engagement with its designated community of records, both creators and users. The proactive outreach and engagement of the organisation with its designated community normally takes place through records appraisal and retention schedules reviews, but because of the challenges of digital preservation, it is advisable that records management staff is involved in additional actions (ISO, 2012). There should be formal agreements and procedures should also be in place in terms of the rights and conditions under which the repository will preserve and allow access to the records, to ensure privacy and confidentiality of such records. Written procedures must be kept in place regarding access to electronic records (Dollar & Ashley, 2015).

Dollar and Ashley (2015) warn that there should be a clear policy that clearly explains the roles, responsibilities, obligations and rights of depositors. There is also a need for agreements between the preservation repository and producers and owners of records.

Depositors must be made aware of what is expected of them right from the ingestion of records throughout to dissemination of information, up until disposition. The organisation should engage users and producers of records within their organisation, not only to establish agreements about rights and responsibilities for transferring records to the repository, but also, to take note of their evolving needs and requirements in terms of digital preservation (Dollar & Ashley, 2015; ISO, 2012).

2.4.1.7 Electronic records survey

Every organisation is responsible for the creation of records regardless of the format or media used. Therefore, they are obliged to ensure the authenticity, integrity and reliability of such records.

One way to maintain the completeness of records is to keep an inventory of electronic records and systems, and to maintain a working relationships between all stakeholders (Altman et al., 2009). The main objective of the records survey is to identify preservation-ready, near-preservation ready and legacy electronic records. Preservation-ready records are those which are in Open Standard Neutral Formats, while near-preservation ready are the ones in formats for which tools are available to export them to Open Standard Interoperable Technology Neutral Formats. Legacy records on the other hand are the ones in formats for which no tools are available to convert them to Open Standard Interoperable Technology Neutral Formats (Idrissi, 2019). Altman et al. (2009) recommend that the electronic records survey should identify the volumes of records which merit long-term preservation and categorise all preservation ready, near-preservation ready, and legacy permanent electronic records. These may include emails and other electronic correspondences.

Normally, a records survey is an organised action that is aimed at locating and identifying all the records that are held by a certain institution. However, there is more to an Electronic Records Survey than just locating and identifying records (Idrissi, 2019).

In digital preservation, the survey includes identifying the media format, type and size (Altman et al., 2009).

Idrissi (2019) affirms that an Electronic Records Survey is normally done to help in the collection of information about electronic records as both the creator and the repository prepare for transfer.

2.4.2 Adherence of the preservation repository to the accepted operational practices

Preservation repository is defined as an institution that is entitled with storing and maintaining the usefulness of records. However, ISO 16363 states that not all preservation repositories are trustworthy. There are certain standards and specifications which need to be met before a repository is considered trustworthy (ISO, 2012).

A trustworthy repository is one that has the ability to provide reliable long-term access to well managed records to its designated users at that specific moment and in the future. Trustworthy digital repositories could be operating in different forms; some erect physical repositories, while others may choose to manage the intellectual aspects and contract a third-party for storage and maintenance (ISO, 2003).

Regardless of the infrastructure, all trustworthy digital repositories must take responsibility to preserve digital records on behalf of their creators and for the benefit of current and future users. They must have their system designed according to accepted conventions and with adherence to recognised standards to ensure continuous management, access and security of their records (ISO, 2012; ISO, 2003). Furthermore, they must develop methods for the audition and evaluation of their systems to meet users' expectations of trustworthiness. They must also have policies, strategies and performance that can be audited (Dollar & Ashley, 2015).

It is argued that a trustworthy digital repository needs to identify its attributes. Different authors have shed light on different attributes of a trustworthy repository (Altman et al., 2009).

The most important attribute of a trustworthy digital repository is compliance with the reference model for an Open Archival Information System (OAIS). The entire repository system must conform to the OAIS reference model.

The preservation of electronic records will depend on a common understanding with all stakeholders about the actions to be taken and how it must be done. The OAIS model stipulates the framework, as well as approved terms and concepts in the architecture and operations of digital archives. Digital preservation repositories must understand the model and be certain of the conformance of all aspects of the system to these models (ISO, 2012; OCLC &CRL, 2007).

Administrative responsibility is highlighted as another attribute of a trustworthy digital repository. A trustworthy digital repository should prove that it is committed to introducing standards and best practice within its community. The trustworthy repository will meet or go beyond community standards and it will involve external experts in validating its processes regularly (Frank, 2022).

Organisational viability is highlighted as one of the attributes too. A repository that wants to be considered as trustworthy should introduce ways to present itself as viable. It should be committed to the long-term preservation of electronic records and its business practices should be transparent. Such an organisation must have an appropriate level of expertise and it must review its policies periodically (Donaldson, 2020).

In addition, financial sustainability is another vital attribute of a trustworthy digital repository. Repositories must be financially stable, with a sustainable business plan in place, both short- and long-term. Furthermore, they must have operating budgets and their financial fitness should be reviewed at least every year (Corrado, 2019).

Equally important, security could be another attribute. It is urged that measures must be in place to ensure the security of digital records. Policies should be implemented to regulate privacy, confidentiality and every other rights of the records. The repository must have disaster preparedness plans and systems which are able to detect any changes in data to protect the metadata of records (Dryden, 2011).

The following are components of the digital preservation repository for a more detailed discussion:

1. Open Standard Technology Neutral Formats
2. Media/Device renewal
3. Integrity
4. Security
5. Preservation metadata
6. Archival storage

2.4.2.1 Open standard technology neutral formats

An effective digital preservation programme should ensure access to readable, authentic and reliable electronic records, which can only be done through the mitigation of file formats obsolescence (Rosa, 2017).

Three related actions are involved in mitigation of file format obsolescence. The first one involves supporting a watch programme on the sustainability of file formats (Saini, 2018).

The second one requires the preservation repository to utilise Open Standard Technology Neutral File Formats for preservation because such formats are hardly dependent on technology. Organisations can also collaborate with records creators to advise them to adopt the use of preservation-ready formats when they create records for long-term or permanent preservation purposes (Rosa, 2017).

Equally important, it is recommended that the repository adopts as many open standard technology neutral formats as preferred digital preservation formats, as possible. It is further advised that the repository keeps monitoring and identifying any other new OS/TN formats before adopting them as suitable to be used as preferred formats (Smallwood, 2013; Idrissi, 2019).

2.4.2.2 Media/Device renewal

No storage medium or device is immune to obsolescence. All digital devices and storage medium eventually decay or go obsolete. Therefore, institutions trusted with the preservation of electronic records with long-term or permanent values must ensure that the information in electronic records remains readable for as long as it is needed (Abrams, 2005).

ISO 14721 clearly states that a trustworthy digital repository should occasionally monitor and renew its storage devices and media to ensure that information is still readable over time.

It is advised that a trustworthy digital repository must have a strong storage device and media renewal programme to renew media and devices which need to be renewed and make sure that they are readable with latest technologies because obsolescence is inevitable (ISO, 2003; Dollar & Ashley, 2015).

An effective media or device renewal programme is described as the one that always keeps inspecting for possible loss of readability of the electronic records and replaces the media automatically. Given the fact that all storage media can go obsolete, it may seem that the only way for repositories to be trusted with long term preservation, is to keep monitoring the readability of their storage media or devices. It is therefore recommended that a trustworthy repository should have in place, a protocol for constantly monitoring the readability of devices (Abrams, 2005).

2.4.2.3 Integrity

Integrity could be defined as the potential of loss of physical and intellectual information after the creation of a record. Digital preservation is a complex process. During this process, records go through different phases, some of which may cause harm or loss of physical and intellectual information.

In order for an institution with a mandate of preserving long-term and permanent electronic records to conform to ISO 14721, it must have a mechanism in place to ensure the integrity of records in its custody (ISO, 2003, p. 6). The best way to monitor integrity is through the use of cryptographic hash digest which are digital fingerprints of electronic records in SIP or AIP. Cryptographic hash digests are computed before the electronic record is preserved and after the completion of the digital preservation operation.

Hence, they will be able to identify any change that may have happened during all the processes of digital preservation (Idrissi, 2019).

2.4.2.4 Security

Security is more than just protecting records for their entire lifecycle. It also involves deciding the safest way to dispose records off, when they reach that stage. Digital preservation requires actions which prohibit unauthorised access to the physical repository where the digital content is reserved. Security also involves protecting confidentiality as well as the privacy of records. Security involves having in place mechanisms which ensure the safety of records in the event of any disaster and assuring the continuity of business in such a case (Dollar & Ashley, 2015).

There should be firewalls in place to protect the security of the records, but back up and disaster management or recovery plans are just as vital. Having in place a written disaster preparedness and recovery plan is necessary as it aids in reducing risks and also decreases liability. It would mean that required data would remain accessible in the event of a disaster, thereby ensuring a continuous flow of information across the organisation (ISO, 2003).

Unlike paper records which are secured by physical locks, electronic records are preserved in systems, and if no appropriate security measures are in place, anyone with a computer could possibly access them. It is therefore recommended that access should be regulated to allow access to authorised personnel only (Ngulube & Adu, 2016).

The server room acts as the actual preservation repository because that is where the actual equipment and technologies which run the system are.

Not only should it have a regulated entrance, but it should also possess every other security measure to make sure that it is safe from not only unauthorised entry, but also to prevent and act in the event of an emergency. It is recommended that security protection processes must be regularly monitored and revised, due to the ever-changing technologies and business needs. (Dollar et al., 2014).

2.4.2.5 Preservation metadata

Preservation metadata is defined as information that supports and documents the process of digital preservation. Metadata determines the integrity of a record. Unless a record is captured with its full metadata that is complete and unaltered, such a record has no integrity and cannot be considered reliable (Dollar & Ashley, 2015, p. 33). It can be categorised into four aspects, namely, descriptive, structural, technical and administrative metadata. Descriptive metadata provides intellectual information such as the author and the title. Structural metadata involves the capture of physical structures such as images and page numbers. Technical metadata provides information about the software and hardware, image sizes and recording lengths. Administrative metadata on the other hand includes information about the provenance (Dappert & Enders, 2010).

A digital preservation repository gathers and keeps metadata that explain preservation processes and actions related to the custody of permanent electronic records. The system must be able to automatically detect any changes in the metadata of a record throughout the entire preservation process and assuring that they remain intact (Bunawan & Nordin, 2015).

2.4.2.6 Archival storage

This is the actual preservation environment and the collections it holds. The archival storage refers to the physical preservation repository and the electronic records held in it.

The ISO 14721 Open Archival Information System Reference Model proffers that there are different automated storage systems which allow the transfer of Archival Information Packages (AIPs) from ingest to the creation of Preservation Description Information (PDI) with the assurance that no corruption has taken place and metadata remains intact (ISO, 2003).

Electronic records may go through multiple processes and stages including changing of formats, different cases of geographically separated storages, and the production of Dissemination Information Packages (DIPs) (Idrissi, 2019). All these processes may lead to a loss of integrity of records. Therefore, it is the responsibility of the institution involved in storage and its stakeholders to make sure that no information or metadata is lost throughout these processes. This is why archival storage is dependent on other preservation services (Dollar & Ashley, 2015).

Digital preservation repositories should at all costs avoid archival storage media which are primitive. Every media is prone to deterioration, but some are too sensitive and they could be ruined easily (ISO, 2003).

It is advised that an institution trusted with the long-term preservation of electronic records must have more than one instances of the preservation repository which supports the storage of AIPs and they should be geographically separated. An ultimate archival storage should consist of at least two instances of preservation repository capable of storing AIPs.

These instances should not be in the same geographical location (Idrissi, 2019). Equally important, the completeness of records should be verified automatically. This information should then be transferred to PDIs, to form an auditable chain of electronic custody (ISO, 2003).

2.4.3 Safety of electronic records when undertaking digital preservation actions (Digital preservation services)

Digital Preservation Services refer to the most practical of the digital preservation aspects. It involves both the intellectual and technical survival of electronic records together with the efforts and responsibilities of records staff as well as repositories. Besides, it could also refer to all actions by every stakeholder involved, from the deposition of the electronic records, their maintenance, storage as well as the media (Ruusalepp & Dobreva, 2015).

It involves actions to ensure not only the security of records, but also their integrity, usability, trustworthiness and accessibility, which is ensured by the preservation of metadata. Above all, digital preservation services are a collective collaboration of stakeholders in assuring the safety of electronic records throughout their entire cycle (Altman et al., 2009).

Discussed hereunder are the two components of digital preservation services:

1. Ingest
2. Access

2.4.3.1 Ingest

Ingestion involves the act of depositing records into the repository by records creators, and the repository accepting such records.

An organisation that is trusted with the preservation of electronic records with long-term and permanent values must be capable of receiving and accepting electronic records from records creators (Smallwood, 2013).

It is a stage that should include efforts from both the producers and the repository. The repository plays the bigger role of making sure that there are agreements between them and the producers, in terms of the formats of records being deposited, integrity, virus checks, metadata and quality. Producers on the other hand should make sure that they adhere to the terms and conditions as per all the agreements with the repository. The preservation repository receives Storage Information Packages (SIPs) from records creators. They are then required to verify the content and integrity of these SIPs. The SIPs are then checked for viruses. Their content and formats are examined too (Ruusalepp & Dobreva, 2015).

These records are then changed to appropriate formats and their metadata is transferred from SIPs into what is called Preservation Description Information (PDI). Archival Information Packages (AIPs) are then created, before the AIPs get transferred to the repository for storage (Smallwood, 2013). The most effective way is to make sure that SIPs are ingested automatically, and the system automatically verifies the completeness of metadata in terms of Administration, Technical, Provenance, Content Description, and Preservation Description significant properties (Dollar & Ashley, 2015).

2.4.3.2 Access

The main aim of the entire process of digital preservation is to make sure that electronic records are readable, authentic and trustworthy, but most of all, accessible. Eventually, users should be able to access the information contained in records.

It is urged that institutions in the business of preserving electronic records should be able to not only make sure that such records remain accessible for as long as they are needed, but also allow users access in the most appropriate and easiest platforms possible (Matusiak, et al., 2017).

Such information is normally accessible as Dissemination Information Packages (DIPs) copied from AIPs, which should be produced automatically, through an integrated search functionality.

This is basically done to regulate access in order to protect privacy, confidentiality and other rights as no user has direct access to AIPs or PDIs. Information searched for by users could be used to audit the production of DIPs (Dollar & Ashley, 2015; ISO, 2012).

2.4.4 Roles of producers and users in digital preservation

Producers are some of the very important stakeholders in digital preservation. Not only do they play an important role as creators and owners of the records, but they are also entitled to selecting the most appropriate repositories to deposit their records into (Sitting & Singh, 2012).

Besides, producers are involved in almost every action with regards to the preservation of records. As owners of records, they have the rights to give terms and conditions of accessing specific records. Producers may, however, require informed advice on some of the technical issues involved in digital preservation. Producers normally submit their records as SIPs which are later transferred to PDI. It is thus the responsibility of producers to ensure that no damage is made to data throughout those processes. They may also receive advice on the most appropriate formats for their records.

In most cases, they are advised to submit their records in preservation ready formats. They are also entitled to set terms and conditions under which their records will be preserved and in determining their retention period. Records would probably be useless if they were not used, because their existence would be of no use. Users are the designated community of the digital repository. They are the end users of the electronic records. It is thus up to repositories to make sure that their records are accessible to their designated users and that they are available in appropriate and usable platforms, while making sure that no access rights of any record is violated in any way (ISO, 2003; Dollar & Ashley, 2015).

2.5 Chapter summary

Although nothing much has been written specifically on the issue of Digital Preservation Maturity, many writers have written a lot on digital preservation in general. Most of the authors have described digital preservation as a complex process that requires serious inputs from all the stakeholders in order to reach an ultimate goal, which is to preserve and provide access to electronic records which are among other things, authentic, useable, complete and trustworthy. Digital Preservation Infrastructure, Digital Preservation Services, Digital Preservation Repositories, as well as Producers and Users have been identified as the most important components of digital preservation. These components and other aspects under them are different, but interlinked and dependent on each other in the preservation of electronic records with long-term or permanent values. It is explained that not all digital preservation repositories are trustworthy, and criteria for a trustworthy digital repository has been detailed (Brown, 2013; Dollar & Ashley, 2015; Dollar et al., 2014; Ruusalepp & Dobreva, 2015.; Altman et al., 2009; ISO, 2012; OCLC & CRL, 2007). The next chapter discusses the methodology for the study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Methodology is the general approach that is taken to the research process. It implies more than just the method a researcher intends to use for the study. It considers the methods that are intended to be used to collect data (Muray & Hughes, 2008).

This chapter discusses the methodology that was used for this study, and it is arranged and organised in sub sections. The first section describes the plan for studying the research problem, the research design. It explains how this study is designed. Data collection methods then follow in which the methods used in collecting data for this study are explained and the reasons as to why such methods were preferred over others. The population is then defined and the methods used to choose the sample from the population are mentioned with reasons why they were the most suitable ones over others. The instruments used during this study are also detailed in this chapter and what makes this study reliable and valid is also explained. Procedures used in conducting this study are then explained and how data were analysed.

3.2 Research paradigm

Research paradigms are consolidated collections of considerable concepts, variables and problems, attached with compatible research approaches and tools (Kivunja & Kuyini, 2017). A paradigm includes the methodology, approach, ontology and epistemology to conduct research. A single paradigm can have more than one methodology, thereby leaving it up to the researcher to follow any of them (Kivunja & Kuyini, 2017).

Depending on whether research is being conducted in pure sciences or social sciences, there are four to five paradigms which are accepted internationally. However, some of these paradigms are barely used. Ontology focuses on the existence of knowledge on a specific subject. Epistemology is a belief of the known and it focuses on how knowledge is acquired and from which sources. It is important because it shapes the researcher's quest for knowledge (Al-Ababneh, 2020).

The essential elements of ontology and epistemology of this study evolves around the interpretivist paradigm. The interpretivist and positivist are the most popularly used of all paradigms. Given its methodology and objectives, this study adopted an interpretivist paradigm. Interpretivism is mostly based on qualitative research. It highlights that social truth is seen and interpreted by people depending on their ideologies. It believes that reality has different layers and it is too complex, hence a single phenomenon can possibly have more than one interpretation (Pham, 2018).

The interpretivist paradigm allows researchers not only to describe, but also to deeply understand the complexity of a phenomenon in its own context, as opposed to attempting to generalise it. The main objective of this study was to assess the Digital Preservation Maturity of the Office of the Prime Minister. Data were collected and analysed by methods which allowed the researcher to make sense of views and opinions of different participants on the issue of digital preservations (Rehman & Alharthi, 2016; Kivunja & Kuyini, 2017).

The interpretive paradigm proven to be the most appropriate for this study because it allowed the researcher to understand and make sense of the complex issue of digital preservation through the interpretations, experiences and opinions of participants.

The researcher made conclusions from those experiences to understand the data collected (Thanh & Thanh, 2015).

3.3 Research approach

Research approach refers to the whole strategy that the researchers opt to use in integrating different components of the research in a logical and consistent way (Myers et al., 2010). It explains a specific plan for studying the research problem. In addition, it provides the researcher with the structure of the research, which the researcher then uses in determining the best way to approach the study. It is further declared that the type of study to be undertaken by the researcher is explained through the research approach. There are three types of approaches to research, namely the quantitative, qualitative and mixed method approach (Maree, 2013).

Qualitative research aims at gaining a comprehensive understanding as opposed to a surface description of a phenomenon. It allows the researcher to gain insights and explore how deep, rich and complex a phenomenon is (Roller & Lavrakas, 2015).

The current study made use of the qualitative approach within the interpretive paradigm, utilising interviews, observation and document review as data collection methods, in investigating the effectiveness of the EDRMS as a digital preservation programme. The qualitative methods of data collection allowed the exploration of views, beliefs and opinions of participants on digital preservation, specifically the effectiveness of EDRMS. It also provided a deeper understanding of the topic than it possibly would with any other approach (Maxwell, 2012). In addition, it allowed the researcher to derive and present easily understandable information and conclusions from the complex issue of digital preservation through detailed and narrowed down information themes.

3.4 Research design

This study adopted a case study research design. A case study is a research strategy and an empirical enquiry that investigates a phenomenon within its real-life context (Bloomfield & Fisher, 2018).

The case study focused on the OPM as it is the institution responsible for the implementation and maintenance of the EDRMS, a programme that is aimed at managing electronic records of the public sector of Namibia. Being the implementer of the EDRMS, the data collected from different departments of the OPM allowed the researcher to deeply understand the EDRMS programme as a digital preservation initiative, from different levels of the organisation and how different aspects of digital preservation affect its effectiveness (Ridder, 2017).

Even though the study focused on the OPM, results created by this study could be useful for any other institution involved in digital preservation in assessing the effectiveness of their digital preservation programmes.

Maxwell (2012) argues that a case study design makes provisions for proving how a specific model or theory applies situations in real life. In that regard, it allowed the researcher to assess the effectiveness of the EDRMS against the criteria of the DPCMM.

3.5 Study population

A study population is generally a big group of individuals or objects that are known to have similar traits or belonging to a similar and specific area of interest which are the main focus of study or research (Mack et al., 2005). This study was conducted at the Office of the Prime Minister of Namibia.

Being on digital preservation, the population was defined by the individuals involved in the entire process of the preservation of electronic records with long-term or permanent values across the organisation. Therefore, all staff members involved in the EDRMS from all 12 departments of the OPM, constituted the population of this study.

3.6 Sampling

Due to the large size of the population, the researcher was not able to gather information from every individual in the population, as it would be expensive and time consuming. Therefore, the researcher relied on sampling techniques. As defined by Dudovski (2009, p. 7), a sample is a part of the population that is scientifically drawn from the entire population of the study to represent it.

This study made use of non-probability sampling techniques, specifically the purposive and snowball sampling techniques. The OPM is the institution that is responsible for the implementation of the EDRMS. For that reason, the researcher applied the census technique to sample all seven (7) employees of the OPM, EDRMS Division to be specific, as the members of staff that could give overall information about the EDRMS programme.

Being in the host division, these professionals were deemed to have information related to not only policies and strategies, but also the functionality of the EDRMS, maintenance and security.

In addition, employees of the EDRMS department would know staff members from other departments within the OPM who are involved in EDRMS. They would therefore refer the researcher to other staff members who represent their respective departments in EDRMS and should be in possession of relevant information.

The snowball sampling technique was used in such a way that the head of archives (Chief Archivist) would refer the researcher to at least two (2) staff members from each of the twelve (12) departments, who are representatives of their respective departments in EDRMS.

The sample consisted of among others, Directors, Heads of Departments, Chief Archivist, Senior Archivist, Archivists, Assistant Archivists, System administrators, IT Technicians, Office Administrators and Records Clerks. The sample was constituted as follows:

- OPM EDRMS Division - Seven (7) participants
- The rest of the OPM - twenty-four (24) participants

  Total = Thirty-one (31) participants

3.7 Data collection methods

This study used interviews, observation and document review as data collection methods. These methods are discussed as follows:

3.7.1 Interviews

An interview is a qualitative method of inquiry that consists of key questions which help to expose the area of exploration, thereby allowing interviewees to respond in more details (Gill et al., 2008, p. 2). In most cases, the interviewer is a researcher or an expert in the subject matter, with an intention to understand the views and opinions of the participants on the subject, through a round of questions and answers (Archibald et al., 2019). The accuracy of information collected through interviews depends on the set up and handling of the interview. Structured, semi-structured and unstructured interviews are the three known types of interviews in research (Gill et al., 2008).

This study made use of semi-structured interviews as one of the data collection methods to make sense of the views, feelings and opinions of the participants on digital preservation in general and the EDRMS as a digital preservation programme. Semi-structured interviews are more flexible as opposed to structured interviews, and as such, they allow the interviewee to discover and elaborate on information which the interviewer may not have previously thought as important.

The interview consisted of open-ended questions, thus leaving room for the respondents to detail and explain their responses, as well as for the researcher to pose follow-up questions.

Semi-structured interviews were considerably flexible and they offered the researcher a sufficient amount of freedom to dig for the deepest thoughts and opinions of the participants on digital preservation and the EDRMS (Adhabi & Anozie, 2017).

3.7.2 Observation

As the name implies, observation is a method of collecting data through observing and taking a record of the behaviours of participants within their contextual settings. This study adopted non-participant observation. The observation was useful in seeing and examining the participants' different roles and activities involving the EDRMS and the management of electronic records in general, with the researcher not necessarily participating. In addition, the observation allowed the researcher to witness first-hand the activities, roles and behaviours of participants, which provided the researcher with important insights and a deeper understanding of individuals and activities involved in the daily management of electronic records (Maxwell, 2012).

Equally important, this method also proved useful in substantiating and adding to the data collected through interviews. Among others, observed were: the appropriateness of the security measures; users' ability to use the system; users' access to the information stored on the system; the system's ability to detect loss of readability or corruption, as well as the Types of formats allowed/accepted by the system.

3.7.3 Document review

This is a data collection technique which involves identifying, examining and analysing documents which are in existence and relevant to the research topic. Reviewing existing documents helps the researcher to understand the history, philosophy, and operation of the programme being evaluated and the organisation in which it operates (Mwita, 2022).

The researcher identified documents which were deemed relevant to the implementation of EDRMS, its use and maintenance and hoped to review and examine among others, agreements, drafts of policies, policies and/or other documents related to the EDRMS and the management of electronic records. However, due to the secrecy of the government the researcher was allowed access to limited documents. The researcher only managed to review some minutes and agendas of meetings related to the implementation of EDRMS and reports on the EDRMS.

3.8 Data collection instruments

This study utilised the following instruments in the collection of data:

3.8.1 Interview guide

With interviews being one of the data collection methods, the researcher developed a tool to guide in the posing of questions.

In addition, it was important to explore the views and opinions from different levels and perspectives of the OPM staff members. Therefore, interview guides used were different. The following semi-structured interview guides were set:

- Interview guide for the Head of Records/Archives
- Interview guide for the Records and Archives staff
- Interview guide for the IT staff
- Interview guide for users/producers

3.8.2 Observation checklist

Observations was also one of the data collection methods as previously discussed. In this regard an observation checklist was used as an instrument. It consisted of items that the researcher deemed crucial to observe and it guided the researcher throughout the entire observation session.

3.8.3 Document Review Checklist

The document review method was aided by the use of a document review checklist. The checklist consists of all the documents the researcher indented to review with regards to the implementation of the EDRMS at the OPM. Items on the list were ticked of depending on whether or not the documents were available for reviewing.

3.9 Reliability and validity

Many researchers have had their say on the issue of reliability and validity from quantitative approach perspectives. This is because these concepts were originally only used in quantitative research.

According to Price et al. (2015), to get a better understanding of reliability and validity, it is important that various definitions of these terms are presented as per different perspectives of quantitative researchers. Some authors believe that since the reliability issue focusses on measurements, then it is not relevant in qualitative research. Paula and Priest (2006) report that reliability and validity are terms that are popularly known within the quantitative type of research, an area in which reliability is defined as the extent to which results are consistent over time. Validity on the other hand is defined as the extent to which a concept is accurately measured. Golafshani (2003) insists that quantitative research ensures an accurate representation of the entire population, and the ability of the study to reproduce similar results under the same methodology.

However, Noble and Smith (2015) believe that reliability and validity are important terms of both quantitative as well as qualitative research, but they need to be measured differently from the two perspectives. Golafshani (2003) stresses that while reliability and validity are used in measuring quality in qualitative research, qualitative researchers should consider the terms credibility, neutrality, consistency and transferability as important aspects for quality.

According to Maree (2013), reliability in qualitative research can be ensured by trustworthiness. Maree further advocates that the quality of research depends on the generalisability of the results. Paula and Priest (2006) suggest that validity in a qualitative research design may refer to the extent to which the interpretations have a common meaning for both participants and the researcher.

In this study, the key mechanism used in ensuring reliability and validity includes the comparison of data collected through two different methods.

Data were collected through semi-structured interviews from the Head of Archives, technical staff of the EDRMS Division of the OPM, as well as users of the EDRMS from different departments. These interviews collected data through open ended questions which required answers with room for further explanations and clarification on the issues surrounding the topic of digital preservation. To ensure trustworthiness of this research, non-participant observation was done, supplemented by document review. The use of these multiple methods increased reliability and validity of the study (Maree, 2013).

3.10 Data collection procedure

Before the researcher could start with the collection of data, a letter was written and addressed to the Executive Director (ED) in the Office of the Prime Minister (OPM). The aim of the letter was to seek permission to conduct research at the institution. Accompanying that letter was another letter from the researcher's supervisor, confirming the researcher's identity and also requesting permission for data collection. Attached to these letters were a copy of the researcher's identity document, proof of registration at the university, as well as a copy of the research proposal with clear insights of what the intended study was about. Within a week after the researcher had written to the OPM, the Executive Director of the OPM responded in the form of a letter, granting the researcher permission to go ahead with the study.

In the meantime, the researcher had applied for an ethical clearance certificate from the Ethics Committee of the University of Namibia. Given the processes involved, the issuing of the ethical clearance certificate was delayed by over eight (8) months since the initial submission of the application, but the certificate was eventually issued.

After receiving the ethical clearance certificate, the researcher then began with the preparations to collect data. Before collecting data, the researcher sent out consent letters to the selected sample. The consent letters were meant to inform participants of what the study is about, what their rights are, and what is expected of them should they agree to participate in the study. Participants were expected to sign these letters if they agreed to participate in the study. After the consent letters were signed, the researcher started making appointments to conduct interviews.

The appointments were made through the EDRMS Division of the Office of the Prime Minister. Meanwhile, the researcher had arranged with the Chief Archivist in the Office of the Prime Minister to gather and allow access to documents that the researcher intended to review. After the reviewing of documents, interviews commenced as per the appointments earlier made.

Interviews were conducted in the participants' respective offices. Having already been introduced through the consent letters that participants had signed, the researcher made an oral re-introduction before starting with the actual asking of questions. Participants were also reminded of their rights and obligations. Equally important, the researcher sought permission from the participants to use a recording device (Phone) to record the interview, to which a majority of participants objected. The researcher therefore, had to take notes as an alternative to the use of a recording device. Moreover, the researcher verbally expressed gratitude to all participants. They were also informed that the observations would begin right after the interviews.

3.11 Data analysis

Data analysis is a systematic process that involves applying statistical and/or logical techniques to make explanations, descriptions, illustrations, revision as well as evaluation of data. It is the process of evaluating data using analytical and logical reasoning to examine each component of the data provided (Thorne, 2000, p. 69). The process of analysing data reduces the amount of information collected, identifies, selects and groups categories together and seeks some understanding of it (Noble & Smith, 2014).

Data collected by this qualitative study were analysed through the use of content analysis. Data collected through the three methods were compared, classified and put into themes according to the scope of the DPCMM as the tool that was used to assess the digital preservation maturity (Bengtsson, 2016). The data were then presented through descriptive narratives.

Content analysis is applicable for both the qualitative and quantitative approach and it can be utilised in an inductive or deductive way (Drisko & Maschi, 2016). While quantitative content analysis presents facts as numbers or percentages, qualitative content analysis presents data in words and themes, thereby allowing the drawing of some interpretation of the results (Erlingsson & Brysiewicz, 2017).

Content analysis can be applied to any type of written text regardless of the origin of the material, could be interviews, a single written question, questionnaire or observations as well as from pictures and films. In addition, there are no specific rules to be followed (Bengtsson, 2016). However, researchers must bear in mind that the depth of the analysis is determined by the methods employed in collecting data. Having employed semi-structured interviews as one of the techniques to collect data.

This method provided deeper information because the researcher was allowed to deepen the discussion with participants (Erlingsson & Brysiewicz, 2017).

With content analysis, the researcher begins by selecting the content to be analysed, which in this case is the data that were collected through the three methods, namely interviews, observations and document reviews. Units and categories of analysis were then defined (Noble & Smith, 2014).

For this study, categories and units of analysis were influenced by the attributes of the DPCMM, the model that was adopted as a theory by this study. To ensure that all texts are coded consistently, sets of rules for coding were set (Noble & Smith, 2014). This included arranging units according to the previously defined categories (Stuckey, 2015). It also gives an indication of what and what not to be included. The researcher then goes through all three data collection methods and all relevant data are recorded in appropriate categories (Nassaji, 2015).

Even though there are different computer programmes which could be faster, the researcher did the coding manually. This is mainly because the study aimed at assessing digital preservation maturity according to the DPCMM. The model already has attributes according to which maturity in terms of digital preservation is assessed. Therefore, using an automated computer programme to code the attributes could compromise the effectiveness of the assessment as it could miss some attributes of the DPCMM. After coding, the researcher then examined the data that were collected and meaningful conclusions were drawn according to the study objectives (Noble & Smith, 2014).

3.12 Ethical considerations

Ethical considerations form a code of conduct for researchers to adhere to when collecting data (Connelly, 2014). These considerations are put in place not only as protection to the rights of research participants, but also to influence the validity of the study and ensure integrity (Arifin, 2018).

This study was conducted according to the ethical conduct as outlined in the Research and Ethics Policy, and the Regulations and Guidelines of the University of Namibia (University of Namibia, 2013). Particularly, the researcher adhered to the following guidelines:

- Made sure that participation was consensual and consent was obtained prior to data collection and no bribes were in any way offered;
- Maintained academic integrity and honesty throughout the study;
- Ensured the confidentiality of participants and their research data throughout the study; and
- Taken note of and adhered to how long research data should be stored.

In that regard, the researcher applied for ethical clearance from the University of Namibia's Research Ethics Committee (UREC), in accordance with the university's Research Ethics Policy and Guidelines. The application was submitted together with the research proposal with the purpose to give the committee members sufficient information about the proposed study. The aim of this application was to get approval from the committee in terms of ethics, before the researcher could proceed with the collection of data.

As expected, the researcher was granted an ethical clearance certificate, with a reference number FOHM -012-2020, which is an approval and permission to go ahead with collecting data. This certificate was issued on the 9th of September 2020.

In ensuring that participants participated willingly, after having received the Ethical Clearance Certificate from the university, the researcher started with seeking consent from participants. A consent form was sent out to participants, giving them an insight of what the study is about and informing them of their rights and what was expected from them should they agree to participate. To ensure the confidentiality of participants, there were no names that were required on the consent forms. Signatures were instead required as a sign of agreeing to participate in the study. Equally important, for the purpose of further protecting the identities of participants, their names were withheld in the presentation of data.

The researcher rightfully opted to use codes instead. This was done to protect the identity of the participants and ensure utmost anonymity. Moreover, the researcher remained honest and truthful, explaining clearly what the aim of the study was and the researcher made participants aware of all three methods of data collection prior to the actual collection of data.

To make sure that the data collected is utilised only for the purpose of this study, the researcher will shred the papers with notes collected during interviews and observation. In addition, raw data captured in the recording device and saved on the personal computer will also be deleted permanently. Equally important, all notes taken during the document review and observation will be shredded, while the interview transcripts will be deleted permanently.

3.13 Chapter summary

This chapter discussed the research methodology of this study. Firstly, it explained the design of the study, the plan, as well as how it was carried out. Methods utilised to collect data in this study were also discussed in this chapter. Furthermore, the chapter highlighted the population of the study and the techniques employed in selecting the final sample and how they were used. It also mentioned and explained the instruments used in collecting data for the study. The three instruments were briefly described and reasons were also given about their appropriateness and how they were used in data collection.

Issues pertaining to reliability and validity were also explained in this chapter, whereby the two terms were defined and explained, and information was given about how they were ensured.

Moreover, it was explained in this chapter the procedures that were involved in the process of collecting data. Equally important, the chapter highlighted the techniques that were employed in the analysis of the data collected. Finally, ethical values considered by the researcher throughout this study were explained. The next chapter presents the findings of the study.

CHAPTER FOUR

PRESENTATION OF RESEARCH FINDINGS

4.1 Introduction

Defined as the arrangement of information collected through data collection methods in the order and form that it is easily and clearly understood, data presentation involves creatively arranging data in a way that it is easily understandable and can be made sense of (Greetman, 2009, p. 11).

This chapter presents qualitative data collected through the methods of interviews, observation and document review. Data are presented in the form of descriptive narratives, with the use of direct quotes. In order for the related data to be presented together, data collected through the three data collection methods are all integrated within headings and subheadings derived from the research objectives. This chapter is organised according to the themes as informed by the research objectives as well as the DPCMM. The objectives were namely to:

- assess the OPM's digital infrastructure for digital preservation
- measure the extent to which the preservation environment of the OPM adheres to the accepted operational practices as guided by standards;
- establish the extent to which the trustworthiness of Digital Preservation Services is ensured when undertaking business actions, and
- determine the influence of producers and users on digital preservation.

Data were collected mainly through structured interviews, with observations and document review as supplementary techniques.

As explained in the previous chapter, to protect the identities of participants, codes were used instead of their real names and profiles.

4.2 Respondents

With the main objective being to assess the capability of EDRMS in terms of digital preservation, the study targeted the Office of the Prime Minister (OPM) as the main institution that is responsible for the implementation of the EDRMS, its maintenance and use. The researcher had initially sampled thirty-one (31) participants. However, due to reasons ranging from Covid-19 restrictions and fears, to unwillingness of some staff members to participate, the researcher could only reach twenty-one (21) participants.

Four sets of interview guides were prepared and in total, twenty-one interviews were carried out with different participants at the Office of the Prime Minister. In the EDRMS Division of the OPM, data were collected from the Heads of Records Management function, Records Management staff as well as IT officers. In the rest of the OPM departments, data were collected from individuals who were selected as representative of their respective departments in the EDRMS programme, who participated as users and producers. Even though four separate interview guides were used, all questions were tailor made to tackle the above-mentioned issues from different angles and perspectives.

To ensure confidentiality as well as protect the identities of the participants of the study, the researcher made sure that the names of participants are withheld by using codes instead.

Respondents per category and how they are coded			
Heads of Records Management function	**Records management staff**	**IT personnel**	**Users and producers**
A1	B1	C1	D1
A2	B2	C2	D2
		C3	D3
			D4
			D5
			D6
			D7
			D8
			D9
			D10
			D11
			D12
			D13
			D14

Table 1: Study participants

4.3 The commitment of the OPM, sustainability and adequacy of its resources

The aim of this objective was to investigate and assess the sustainability and adequacy of the infrastructure involved in the implementation, use and maintenance of the Digital Preservation programme, which in this case was the EDRMS at the OPM. With this objective, the study also sought to determine the efforts and commitment of the OPM, through its resources, in ensuring the effectiveness of the EDRMS.

The results are presented in the following sub-themes:

- Digital Preservation Policy
- Digital Preservation Strategy
- Governance
- Collaboration
- Technical expertise
- Designated community
- Electronic records survey

4.3.1 Digital Preservation Policy

As it is the case in managing any other affair, adopting a policy is vital in managing electronic records, because it sets guidelines which influence decision making (Rosa et al., 2017). In this regard, respondents were asked about the availability of a Digital Preservation Policy. The responses show that the EDRMS was implemented with no digital preservation policy in place. All the respondents confirmed that there was no digital preservation policy.

For instance, A1 responded; “No, there is no policy as far as digital preservation is concerned.” A2 also confirmed by saying that; “No, not that I know of. If there is any, then it is may be with the developers of the system, because the system was not developed in Namibia.” Similarly, C1, C2 and C3 all indicated that there is no digital preservation policy in place. For instance, C2 stated that, “I am not aware of such a policy.”

Some participants could not differentiate between a digital preservation policy and the Archives Act. For example, B1responded, “I know there is a National Archives Act, but I do not know of a digital preservation policy or maybe it is the same thing” However, A1 revealed that there is a draft digital preservation policy by stating that, “We however have a draft from 2017, but it is not yet formal.” The researcher, through the process of document analysis has confirmed that there is indeed a draft of a policy.

It may seem as if the OPM was not the one with the responsibility of implementing the policy, as noted by A1, who stated that, “It is the responsibility of the National Archives of Namibia, as the body responsible for the management of records and archives, to come up with that policy. I believe they were instructed to do so.” Moreover, A2 insisted that, “I believe the National Archives should come up with the policy, because it is within their mandate.” Some participants claim that it is the responsibility of the National Archives of Namibia to implement the digital preservation policy. However, both the observations and analysis of documents done by the researcher could not find any evidence to substantiate such claims.

When the researcher posed a follow up question; “Are there any plans to come up with a digital preservation policy?” most respondents indicated that there seems to be no plan of coming up with a digital preservation policy any time soon.

According to A1, “I am not aware of plans to come up with a digital preservation policy any time. Even the draft that is in place, I do not see it being reviewed any time soon.” However, the response from A2 showed a little hope, by stating that, “I am hopeful that this policy will be implemented soon.”

The unavailability of a digital preservation policy tempted the researcher to investigate any possible complication. Therefore, a follow up question was then posed, “Does, not having a digital policy affect you in any way?” According to the responses, most participants were at least aware of some of the dangers of operating the EDRMS without a policy. For instance, A1 responded that, “I believe a policy will help guide us in everything that has to do with the management of electronic records. Maybe it will give us rules and regulations about what is allowed and what is not.” A2 asserted that, “I believe a policy is important. Now, we just operate and do everything on our own, nothing is guiding us. I do not even know what will happen if something goes wrong with these records.” Observation and document review have also concluded that there is indeed no digital preservation policy at the OPM.

4.3.2 Digital Preservation Strategy

In Digital Preservation, it is important to have a strategy which clearly indicates how the organisation can reach its goals (Ashenfelder, 2017). To gather information on the Digital Preservation Strategy, the following question was posed: “Does the organisation have a formal strategy that addresses technology obsolescence?” Responses indicate that there is no formal strategy in place to address technology obsolescence. A2 said, “Not that I am aware of.”

Furthermore, there was no indication that participants were aware of the link between the digital preservation strategy and the policy. This came out in A1's response that, "No, I think that is supposed to be part of the policy, which we currently do not have."

Also, there seemed to be some confusion about who the strategy applies to. This could be confirmed from B1's response that, "I am not aware of any formal strategy to tackle that.

The system is monitored by the IT personnel who are responsible for the technical part and they are the ones responsible for monitoring technology obsolescence." In much the same way, B2 appraised that, "There is no formal or written strategy, but System Admins are required to upgrade the system to the newest version available."

Asked if they were aware of any strategy in place that addresses technology obsolescence, C1 said, "If there is such a strategy, then it was probably not communicated to us." C2 affirmed by saying that, "No, unless I am not aware of it." C3 was also not aware of any strategy and responded that, "I am not aware of any strategy."

With a clear indication that there was no strategy in place, the researcher posed another question, "Are changes in technology being monitored?" All responses were almost the same, indicating that even though there was no formal strategy to guide in monitoring changes in technology, the system was always updated. For instance, C1 claimed that, "We do monitor, manually. Only when, maybe if there is a change in windows and everything related to that and then we upgrade." C2 affirmed by saying that, "We try to keep updating the system to the newest version available, but we do it manually." C3 also alluded that, "If you are asking if there is a strategy in place for that, then its no. But, we do check if there is any software that is outdated so that we can update it."

4.3.3 Governance

It would be impossible for any organisation to operate without governance. Governance involves more than just controlling. It includes issues of compliance, accountability and administration, to mention the least (Brooks, 2019).

Seeking information on that subject, the researcher asked the question, “Is there any formal information on governance which assigns accountability and authority for digital preservation?” Responses from both A1 and A2 have shown that there was no formal information governance in place. A1 responded that, “Apart from job descriptions, there is no other.” On the other hand, A2’s response indicates an understanding that governance should be part of the policy, by explaining that, “No, the issues of accountability and authority are supposed to be part of the policy. Not only for the EDRMS, but a national policy.”

Another question was posed; “Is there any framework to ensure compliance of preservation repository, with applicable laws, regulations, records retention schedules, disposition authorities and standards?” All responses have shown that there was no governance framework to ensure compliance to applicable laws and electronic records management best practices. For instance, A2 responded by saying, “In terms of EDRMS, I do not know any framework.” A1 responded that, “The only document we have is an approved file plan, according to which we used to file our paper records. I am not sure if it is applicable to the management of electronic records.”

Some responses have shown that most of the records management tools which were in place only catered for manual records management and not for electronic records.

In that regard, A2 gave a brief explanation on the absence of the framework and gave reasons as to why there was no such a framework in place. Light was also shed on the importance of reviewing current policies and regulations to be able to cater for electronic records. According to A2:

> *"We currently just adhere to the Archives act, which unfortunately only caters for the management of manual records and not for electronic records. There is a need for these acts to be reviewed and come up with a new policy which will accommodate the management of electronic records."*

Similarly, Respondent B1 shed some light on the availability of an approved File Plan, which also only catered for manual records management, by saying:

> *"The only tool available in terms of disposition authority is a file plan. The filing system clearly indicates all applicable laws around retention, disposition and other standards. But I think it cannot be used for the EDRMS, because it was created for paper records and the EDRMS has electronic records."*

B2 affirmed that, "We do not have any framework in that regard." With all responses indicating that there was no governance framework in place, the researcher asked if there was any plan to come up with one. All answers indicated uncertainty in terms of plans to implement a governance framework.

However, respondent A2 expressed some hope by saying that:

> *"I am not aware of how far the preparations are, but I hope that a policy is implemented now than later, because I believe that all those issues should be part of the policy. If we can start by reviewing the draft we have, then it will be easier. I am hopeful that we will have something in place soon."*

4.3.4 Collaboration

Digital Preservation is broad and requires advanced technology and expertise among other things. Without collaborating, individual organisations may have difficulties ensuring effective electronic records management. For this reason, collaboration may come in handy (Pinnick, 2017). To gather information on this specific subject, the researcher posed this question: "Does the organisation have in place, a framework that allows it to collaborate with standing partners?" Respondent A1 answered shortly saying, "There is no such a framework in place. We have our own people on board." Respondent A2 explained a little bit in detail by saying,

> *"No, there is no such a framework in place. We however have the service providers who are the suppliers of the system. If we have issues our team cannot resolve, then we contact them. Other than that, we have our own people within the organisation."*

The researcher then posed a follow-up question, "Are there any plans to collaborate with any other entities in the future?"

Respondent A1 explained that there are no plans on paper, but suggested how they would go about collaborating, saying that,

> *"We do not have a plan written somewhere, but maybe, we just need to identify areas which we may need help in, as far as EDRMS is concerned. From there, we can then identify institutions we can work hand in hand with."*

Even though there were no plans to collaborate, respondent A2 was hopeful and anticipated to work with organisations which are good with technology in future. According to A2, "At the moment, no. But I think we need to work with people who are good with technology. Maybe one day we will have a few institutions to work with."

Asked if they collaborated with any other organisation or entity in terms of electronic records management, all respondents have indicated that they did not collaborate with anyone in that regard. According to B1, "We do not collaborate with any other entity, but the IT people within our organisation, help us with IT issues." In affirmation, B2 responded that "No, we do not collaborate with anyone from the outside, but when we have issues with the system, sometimes the IT people would help us."

On the same subject matter, asked if collaboration would make a difference, respondent B1 raised a need to collaborate, by saying:

> *"We do not collaborate with any entities at the moment, but the system was procured from a foreign company, if I can call that collaboration. I believe it is important that the OPM identifies institutions who are in the same business of electronic records management if there is any, so that we can work with them.*

We may need them one day. The EDRMS is new to us and there are a few things we may need help with."

B2 affirmed that,

"*Yes, I think it would have a big impact. This EDRMS is a new initiative and we do not really know everything. Maybe if we were in collaboration with organisations which have been in this business for longer, we would learn a lot."*

4.3.5 Technical expertise

The success of any Digital Preservation programme depends on the level of expertise involved and the commitment of the organisation in making sure that staff members are equipped with relevant and up to date skills (Aziz et al., 2018).

To gather information on the matter, the researcher asked if there were qualified personnel for positions involving electronic records management. All responses indicated that there were qualified personnel. For instance, respondent A1 responded that, "All our staff members in the EDRMS Division are qualified." A2 claimed that, "In the EDRMS Division, yes." The researcher posed a follow up question saying, "Do your employees have any operational access to specialised professional technical expertise?" According to the responses, it is clear that staff did not have any external operational access to specialised professional technical expertise. However, staff members helped each other when needed, within the organisation.

This was confirmed by A1's response that, "Internally, yes. We have IT personnel who help the other staff with any technical issues with the system."

Likewise, respondent A2 responded that, “We help each other where we can, within our department. Nothing from the outside.” Having learnt that staff did not have any access to external operational access to specialised professional technical expertise, the researcher sought for a deeper understanding on the matter and asked, “What measures do you have in place to make sure that your staff members are up to date with necessary expertise?” Respondent A1 responded that, “Honestly, we have none what so ever, maybe just in their personal capacity.”

Respondent A2 went a little bit into detail and said:

> *“We do not have any measures in place in that regard. I am not so sure whether the government in the current economic state, can even afford to pay for such. But maybe arrangements for training could be made on request, but I doubt. For now, maybe staff members can get training in their personal capacity.”*

Seeking confirmation from staff members, the researcher asked, “Have you ever received any training with regards to electronic records management?” All responses were negative. The researcher further asked, “Do you have any operational access to specialised professional technical expertise?” All responses clearly confirmed that staff members did not have access to external technical expertise. They also indicated that staff members helped each other within the division. For instance, B1 answered that, “No, but we depend on the IT technicians for IT-related issues.” Similarly, B2 said “No, but the IT people help us when we have a problem with the system.”

4.3.6 Designated community

Records would probably be useless in the absence of consumers of the information and other stakeholders. The designated community plays an important role in evaluating the usability of information. The efforts and commitment of the host institution and its stakeholders impacts the effectiveness of digital preservation (Dollar & Ashley, 2015). To gather data in this regard, the researcher posed the following question, "Is there any formal document that defines the rights, obligations and responsibilities of your designated community for electronic records to be transferred to the repository?" All answers were "no", with A1 explaining that, "I think that should have been in the policy, which we do not have at the moment." Digging deeper, the researcher further asked, "Are there written agreements between users, producers and the repository in terms of rights, obligations and responsibilities as far as transfer, custody and dissemination is concerned?"

All responses indicate that there were no such agreements in place. For instance, respondent A1 said, "No, but there are restrictions on who should have access to what." In affirmation, respondent A2 answered that, "No, we do not have any written agreements, but access to the system is restricted." Seeking confirmation from users and producers of records, the researcher asked, "Have you ever signed any agreement with the repository?" All responses were negative. The researcher further asked, "Were you ever engaged by the repository regarding the establishment of any agreement?" to which they all responded negatively.

4.3.7 Electronic records survey

Before implementing any records management programme, a survey needs to be done in order to, among others, identify all the records held by the organisation (Altman et al., 2009).

Collecting data about the electronic records survey, the researcher asked the Heads of the Records Management Function: “Has the organisation ever carried out an electronic records survey?” Both respondents, A1 and A2’s answers were “yes.” The researcher further asked, “How often is it done?” Respondent A1 answered, “Only once in every department.” Respondent A2 explained in detail saying, “We only did it once to verify if different departments, ministries and other government institutions have the required infrastructure before implementing the EDRMS.”

Seeking confirmation from users and producers, the researcher asked, “Have you ever participated in an electronic records survey?” All responses indicated that at least seven of the respondents have never participated in any records survey. The rest of the respondents who indicated to have participated in a records management survey, were further asked, “How many times?” to which they all responded “once.” While analysing documents, the researcher stumbled upon some documents with questions which were used in the records survey.

4.4 Adherence of the preservation repository to the accepted operational practices

This objective sought to establish the extent to which the repository and preservation environment of the OPM adheres to the accepted records management operational practices.

With this objective, the study assessed the adherence of the EDRMS to records management standards as outlined by the DPCMM, from implementation to its daily operation.

The results are presented in the following sub-themes:

- Open Standards Technology Neutral Formats
- Device/Media renewal
- Integrity
- Security
- Preservation metadata
- Archival storage

4.4.1 Open Standards Technology Neutral Formats

It is highly recommended that repositories adapt file formats which are neutral, because such formats barely depend on technology (Saini, 2018). To gather information about Open Standards Technology Neutral Formats, the researcher posed these questions to the Heads of the Records Management function and Records Management staff: “Has the repository adapted any file format as a preferred format?” All responses were “yes.” Seeking for explanations, the researcher further asked, “Which format and why that specific format?” All responses indicated that the repository had adopted PDF as a preferred format. However, respondents had different views as to why PDF was adapted as the preferred format, for instance, B1 said, “Because we normally upload scanned documents, and the scanner automatically saves the document into PDF.”

B2, on the other hand, went a little deeper by saying that, “I believe it is because PDF cannot be edited. The scanners we use also just save the documents into PDF.” The researcher had to seek confirmation from the IT and posed the same question. Respondent C1answered, “At the moment, the system only accepts PDF, but this can be adjusted upon request.” Respondent C2 affirmed that records management staff may have requested for it by saying that, “Yes, PDF. I believe PDF is considered more durable in records management than any other format.”

Respondent C3 explained that the system was made elsewhere by saying that:

> “*Yes, PDF because the system was tailor-made to accept documents in PDF formats only. We are not the creators of the system, but I believe it was done by request. Maybe it is what the Records Managers have required. But if there is a need for any adjustments to be made, we can still do it.”*

The researcher then posed another question, “Is there any technology watch programme in place to monitor the sustainability of that format?” Most participants did not understand what a technology watch programme was. After an explanation from the researcher, all responses have shown that there was no technology watch programme in place. For instance, C1 answered, “No, we do not.” In affirmation, C2 said, “No, not that I know of.” Respondent C3 also indicated that there was no program in place and explained saying, “No, we do not have a formal technology watch programme, but we keep updating the system.” Having been asked by the researcher the following questions: “Are you required to upload your records in a specific format?” and “What is the required format?” all users and producers indicated that they upload their records in PDF.

Most respondents did not have a clue as to why they were required to upload their records in PDF, but some had a few reasons, for instance respondent D9 said, “We upload our documents in PDF because the scanners turn them into PDF.” D12 speculated that, “PDF, maybe because PDF cannot be edited like word.”

It can be concluded from the observations done by the researcher, that records were uploaded in PDF. Equally important, the researcher also confirmed that there was no formal technology watch programme in place.

4.4.2 Device/Media renewal

All storage medium and devices are prone to obsolescence. It is therefore the responsibility of Digital Preservation institutions to make sure that the information remains readable over time (Abrams, 2005). To gather information about Media Renewal, the researcher posed the following question, “Does the repository have a formal media renewal protocol in place?” They all answered “no.” Seeking further information, the researcher asked, “Does the system automatically monitor the potential loss of readability?” According to respondent C1, “Not automatically, but if a record fails to open with the current technology, we update to the latest available.” In affirmation, C2 answered that, “We monitor that manually. Not on a daily basis though, but only if there is a problem with readability. Only then we would act.” Respondent C3 also confirmed that, “No, but we keep updating the system.” Moreover, it was observed that the EDRMS did not automatically monitor the potential loss of readability. However, the IT personnel manually made sure that the system and supporting software were up to date.

4.4.3 Integrity

As it is the case with paper records, electronic records' reliability and authenticity play vital roles in determining their integrity (Idrissi, 2019). To find out about the integrity of electronic records of the EDRMS, the researcher asked, "Does the repository have a documented procedure for integrity protection of electronic records?" From the responses, it is clear that there was no integrity protection procedure that is documented at the OPM. This could be concluded by the responses from A1, A2 and B1 all of who answered, "no." B2 reasoned that, "Nothing. I believe that would have come with the policy." Participants responded as if they did not quite understand the question, therefore, the researcher further asked, "How does the repository ensure the integrity of electronic records throughout all preservation actions?"

In this regard, respondents highlighted that the system assured that the metadata of records were captured entirely and any modifications or changes made to records could be traced. For instance, B1 insisted that, "Information of records is entered separately, manually and records cannot be uploaded to the system if all fields are not completed." Highlighting an audit trail as a security measure, respondent B2 confirmed that, "The system produces history of the movement of every record. You will know who accessed what record and what changes they have made." The researcher further asked, "Does the system generate Hash Digests or how do you detect any possible changes to records?" According to the responses, EDRMS did not necessarily generate Hash Digests. However, the system was able to produce a history trail of the movement of records. In that regard, respondent C1 claimed that, "No, what the system does is produce an audit trail of the movement of records.

Giving information of when it was accessed, by who and any possible change made." In support, C2 affirmed that, "The system only creates an audit trail which is enough to detect any possible change in the record." C3 also confirmed that, "No, the system provides a trail of information about the movement of records. If someone accesses the record and changes something, the audit trail will show." In addition, the researcher confirmed, from observation, that when uploading records to the EDRMS, the user was required to fill in the information about the record, manually. The system could not accept the record until all the fields were completed as required.

4.4.4 Security

To ensure the safety and usability of records for as long as they are needed, security needs to be prioritised. One of the most crucial security tools in records management is disaster preparedness and recovery plan. Seeking information in that regard, the researcher asked, "Does the organisation have a written disaster preparedness and recovery plan?"

According to the responses in this regard, the OPM did not have a disaster preparedness and recovery plan as far as the preservation of electronic records is concerned. However, it may seem as if the only disaster preparedness and recovery plan in place was that of the National Archives, which was implemented for the management of manual records and did not cater for electronic records. This was confirmed by respondents A1, A2, B1 and B2 when they all responded "no", with A2 explaining that, "We only have the one for the National Archives, but it does not cater for electronic records." Having discovered that there was no disaster preparedness and recovery plan in place, the researcher had to ask for information about any measures in place in the case of a disaster, by asking, "What are the measures in place to ensure that no records are lost, in case of any emergencies?"

All responses were directed to the system back-up. For instance, respondent A1 responded: “The system is backed up and there is an offsite storage.” Respondent A2 affirmed that, “The IT have back up.” Respondents C1, C2 and C3 all confirmed the availability of a back-up, with C1 claiming that, “The data on the system is backed up.” C2 stressed that, “Information on the system is safe in the case of any emergency because we have a back-up.”

Attempting to gather information about the availability of other security measures, the researcher further asked, “Are there other measures that are in place to ensure the security of electronic records from loss, theft or unauthorised access?” Most respondents pointed out “passwords” as a security measure.

For instance, respondent A1 answered: “Users have passwords, known only to them and people can only access records which they are authorised to, depending on their positions and departments.” Respondent A2 asserted that, “We have passwords and we can only access some records as authorised.” Similarly, responding to the same question, respondents C1 and C2 had this to say, respectively, “The system has restricted access.

Individuals have passwords and they are only authorised to access some records depending on their authority,” and “Users are assigned passwords which they use to log into the system. Also, some records are only accessible to some people.”

During observation, the researcher identified several security measures, especially in the server room and they were ticked off in the observation checklist as annexed.

4.4.5 Preservation metadata

Metadata plays a vital role in the reliability and completeness of records. It is therefore important to ensure that metadata remains intact throughout all records management actions (Dappert & Enders, 2010). Whilst collecting information about metadata, the researcher posed this question, "How do you ensure that metadata of electronic records remain intact throughout all the preservation actions?" All responses indicated that records' metadata was captured independently and the EDRMS produced a trail of the movement of records. For instance, respondent A1 answered,

> *"Firstly, the metadata is capture manually and separately, so records cannot be uploaded to the system without complete metadata. Also, the system produces an audit trail, with information about the movement of the record and it would detect any change in metadata."*

Respondent A2 confirmed that, "The system captures any changes made to a record and produces a trail." Responding to the same question, the rest of the respondents confirmed what A1 and A2 had already explained.

For example, Respondent B1 responded that, "Metadata is captured manually. There is a form one has to fill before they can upload any record to the system.

All the fields on the form must be completed, if not, the system will not accept the record." In addition, B2 said that, "The system produces an audit trail to any change that may have been made to the metadata." According to C1, "The system rejects any record that has no complete metadata. It also produces an audit trail of the movement of records, therefore detecting any change in metadata."

Moreover, Respondent C2 answered that, “Records background information is entered manually by users. Unless every required information is entered correctly, the system will not accept the record.” Respondent C3’s answer was, “Once the record is captured to the system with all its metadata, its movement is then tracked by the system. A trail of when it was accessed, by who and changes made is produced by the system.” Users were asked if the system could automatically capture metadata or it was entered manually. All respondents claimed that the system allowed for the manual entering of metadata. For instance, respondent D10 said, “No, we do it manually. When uploading a document to the system, we are required to fill in fields of information about the record. It will not go through unless all fields are completed.” D13 affirmed that, “We enter information manually.”

4.4.6 Archival storage

To determine the effectiveness of digital preservation of any institution, one needs to examine not only the preservation repository, but also the electronic records held in it (Idrissi, 2019). Collecting information about what the OPM preservation repository holds, the researcher asked, “Does the repository’s holding consist of any primitive archival storage?” Unsurprisingly, all respondents answered “no.”

The researcher further asked, “How many instances of the preservation repository supports the storage of AIPs?” There was a moment of explanation by the researcher as respondents did not know what AIPs were.

After the researcher’s explanation, all responses indicated that two instances support the storage of AIP. For instance, respondent C1 answered that, “Two, the main one and the one for back up.” Respondent C3 affirmed that, “Two, because we also have back up.”

The researcher further asked, “Are these instances geographically separated?” Respondents C1 and C2 both answered “yes.” Respondent C3 affirmed by saying, “Yes, in case anything happens to either one of them.” Furthermore, through observation it was affirmed that the repository did not hold any primitive archival storages.

4.5 Safety of electronic records when undertaking business actions

This objective sought to establish the extent to which the OPM ensured that electronic records remain safe, secured, usable and accessible when business actions are undertaken. With this objective, the study assessed the efforts of the OPM in making sure that electronic records do not, in any way lose value and integrity, throughout their life cycle.

The results were presented in the following sub-themes:

- Ingest
- Access

4.5.1 Ingest

An organisation like the OPM, which is trusted with preserving electronic records, must be capable of receiving and preserving records for as long as they are needed. Enquiring about ingest, the researcher posed this question, “Does the repository have any agreement with producers in place with regards to the format, integrity, virus checks, metadata checks and quality?” Respondent A1 responded, “No agreement in place.”

Respondent A2 affirmed by explaining that, “There is no agreement in place. Maybe it should have been in the digital preservation policy that we do not have at the moment.” In addition, the researcher sought to understand the role of users in the process of ingesting.

This question was posed by the researcher, “Do you sign any agreement with regards to format, integrity, virus checks, metadata checks and quality?” All users indicated that they did not sign any agreements in that regard.

Trying to establish how the completeness of records was ensured, the researcher asked, “Is metadata checked manually or the system does it automatically?” All responses indicated that even though the system, per se did not automatically check the metadata, it did not accept records to be uploaded unless all the required metadata fields were completed. For instance, respondent B1 said, “It is entered manually but the system checks it automatically.” Respondent C3 affirmed that, “The system does not really check it automatically, but it does not accept records without complete metadata.”

4.5.2 Access

One of the most important obligations of any institution in the business of electronic records management is to make such records accessible to users. With regards to gathering information about access, the researcher posed the following question, “Does the repository allow users access to their records?” As expected they all responded “yes.” The researcher further asked how users are allowed access to their records. According to the responses, the system had a search functionality which users used to locate and retrieve the information.

According to respondent B1, “They log into the system and the system allows them to search for anything they are authorised to access.”

Respondent B2 affirmed that, “They log in with their passwords. They are also allowed to type in the keyword of whatever they are searching for and it pops up.”

Seeking further information from the IT, the researcher asked, “Does the system have an integrated search functionality?” and “How does it work?” According to respondent C1, “Yes, they simply log in, type in any keyword or reference and the system suggests” Respondent C2 affirmed that, “Yes, and they just type in any hint.” Similarly, C3 answered that, “Yes, they only need to type in what they are looking for and it pops up.” Having been asked if they are allowed access to their records, all users responded “yes.”

4.6 The roles of producers and users in the process of electronic records preservation

This objective sought to determine the roles of producers and users from creation, transfer as well as the use of the digital records at the OPM. Producers or creators of records are also the users of such records. For this reason, these two terms are used interchangeably. With this objective, the study could also establish the extent to which producers and users understand their responsibilities, authority and roles both as producers and users of the system throughout the entire process of electronic records management.

Equally important, some roles of users may have already been established and discussed under different themes. It is because of this objective that the study could establish roles of individuals responsible for creating and using electronic records and what is expected of them as far as the entire process of electronic records management is concerned.

Seeking information on issues of authority and responsibility in the process of digital preservation, the researcher posed this question, “Do you understand your authorities and accountabilities both as a producer and a user of electronic records?”

Most respondents responded by saying, “yes.” Some respondents went as far as mentioning a few of what their responsibilities are, for instance, respondent D11 answered, “My responsibility includes scanning and uploading records to the system and retrieving them when I need to.”

D12 affirmed by saying, “I am responsible for scanning paper records and uploading the soft copies to the system. I can also access the records when I need to use them.” Most respondents were however reluctant to shed light on the issue of authority. Therefore, the researcher posed a follow-up question, asking, “Do you play any role in retention scheduling?” Most responses were negative, with most of them highlighting the availability of an approved file plan which already has a retention schedule and disposal guidelines. For instance, respondent D2 said, “The government has in place a filing system which has details on how long records are to be kept and when they need to be destroyed. We work according to it.” D5 affirmed by saying, “Retention scheduling is outlined in the file plan. I do not have any role in it.” Respondent D9 explained in detail, highlighting again the need for a policy, by saying:

> “*Right now, we only have a file plan that was approved by the National Archives of Namibia the time when we preserved only paper records. Now that we have to scan and upload records in an electronic format to the system, I believe that the retention schedule and disposal guidelines should also change. Maybe they are busy with that, I do not know. I think the policy you asked about must also include these things because right now, we only have the file plan.”*

4.7 Chapter summary

This chapter presented data that was collected through interviews, observations as well as the reviewing of documents. Data collected through these methods were integrated under relevant subheadings. The chapter arranged the collected data collected according to themes which were motivated by the research objectives as well as the DPCMM.

To ensure the privacy and confidentiality of participants, codes were used to represent them. No name or any personal identity was revealed in this chapter.

The findings of the study revealed that the Office of the Prime Minister implemented EDRMS without an electronic records management policy in place. In addition, it was revealed that such a policy is supposed to be the responsibility of the National Archives of Namibia and not the OPM.

Moreover, technology obsolescence was not formally addressed due to the absence of a formal digital preservation strategy that would address that issue. As a result, there was also no formal strategy to monitor changes in technology. Instead, the IT personnel kept updating the system in their own terms. The study further discovered that there was no formal Information Governance Framework to assign accountabilities and authorities for digital preservation and to ensure compliance of preservation repository, with applicable laws and regulations, a records retention schedule, and disposition authorities and standards. The chapter further presented that even though participants feel the need to collaborate, there is no formal framework that allows them to collaborate with standing partners and other institutions in the business of electronic records long-term preservation.

Equally important, it was revealed that even though there were qualified personnel in all areas involving records management, the staff members never received any training in terms of electronic records management.

Neither did they have any operational access to specialised professional technical expertise, apart from the IT personnel within their organisation, who would help other staff members involved in records management with IT related issues in their own capacity. According to the results of the study, there was no formal document to define the rights, obligations and responsibilities of the designated community for electronic records to be transferred to the repository.

Also, the repository did not have written agreements with records users and producers in terms of rights, obligations and responsibilities as far as transfer, custody and dissemination is concerned. It was discovered that an electronic records survey was conducted, at least once, with the aim, among others, to verify if different departments, ministries and other government institutions have the required infrastructure before implementing the EDRMS.

The results further revealed that the repository adapted PDF as a preferred format. However, there was no formal technology watch programme that is in place to monitor the sustainability of that format. Moreover, the repository did not have a formal media renewal protocol in place and the system could not automatically monitor the potential loss of readability. Therefore, the IT personnel update and monitor the system manually. In addition, the registry did not have a documented procedure for the integrity protection of electronic records. The metadata of records was entered manually. However, the system did not accept records, unless all fields of information (metadata) are completed.

Even though it did not produce hash digests, the system kept track of the movement of records and produced an audit trail. In terms of security, the repository did not have a written disaster preparedness and recovery plan that caters for electronic records. However, everything on the system was backed by IT. Equally important, access to the system was restricted. Users had passwords and they could only access records which they were authorised to access.

The repository did not hold any primitive archival storage and it had two, geographically separated instances which support the storage of AIPs. In terms of access, the system allowed users access to their records from their computers through an integrated search functionality. The next chapter discusses and interprets the findings.

CHAPTER FIVE

DISCUSSION AND INTERPRETATION OF FINDINGS

5.1 Introduction

According to Muray and Begler (2009), the discussion of the study is done through the interpretation and description of the significance of the research findings in light of the already existing knowledge about the research problem being investigated and to explain any possible new understanding about the research problem after considering the findings. This chapter discusses and interprets the findings of the study, as presented in the previous chapter (Chapter four). It is under this chapter where the findings of the study are detailed, explained and interpreted with reference to the DPCMM theoretical framework and the literature on digital preservation. Moreover, the findings of the study are compared to the literature and evaluated against the requirements of digital preservation maturity, as per the DPCMM theoretical framework. In so doing, all the objectives of the study are fulfilled. As it is the case with Chapter four, this chapter was also constructed based on the objectives of the study.

5.2 The commitment of the OPM and the sustainability and adequacy of its resources in ensuring effective digital preservation

For a clearer presentation of the findings of the study, this research objective is discussed according to the following sub-headings:

- Lack of Digital Preservation Policy and Strategy
- Lack of governance frameworks

- Lack of collaboration frameworks
- Lack of training and limited technical expertise
- Poor consultation with the designated community and insufficient electronic records Survey

5.2.1 Lack of a Digital Preservation Policy and Strategy

The study established that the EDRMS was implemented and was still operating without any Digital Preservation Policy in place.

Noonan (2014) highlights the lack of relevant policies as one of the worst-case scenarios in the management of electronic records. Da Silver and Borges (2017) affirm that in the business of electronic records management, operating a programme without a Digital Preservation Policy is bad practice. According to Noonan (2014), not only does it explain why the chosen electronic records need to be preserved, but the Digital Preservation Policy also needs to pinpoint how the rest of the policies like the acquisition policy will apply to the acquisition and management of electronic records which the archive wants to preserve. Basically, the absence of a digital preservation policy compromises some other important policies of electronic records management. This basically means that the digital preservation policy is the main policy upon which other relevant policies of electronic records management could be based on.

Pinnick (2017) argues that there is a great need for every institution in the business of long-term preservation of electronic records to disseminate the digital preservation policy to all its stakeholders. It is further required that the institution evaluates its conformance to the policy and reports to its governing body. The policy should also be audited and reviewed appropriately.

Da Silver and Borges (2017) agree that users and producers need to understand everything around digital preservation, therefore, they will need a policy to clearly indicate to them how they fit in the whole process of digital preservation.

This implies that in the absence of a digital preservation policy, stakeholders, including users and producers, do not have knowledge of their roles in the entire process of digital preservation. Pinnick (2017) concludes that in the absence of a Digital Preservation Policy, issues of authority and accountability are compromised.

In addition, the OPM did not have a Digital Preservation Strategy in place. According to Dollar and Ashley (2015), Preservation Strategy could be defined as a set of procedures which regulate how the process of Digital Preservation will be supported. This may include what is required of depositors before submitting their electronic records; software emulation and when it may be needed; issues of file formats; monitoring of electronic records to make sure they remain accessible and readable, as well as the process of allowing access to records. According to Blumenthal et al. (2020), a strategy in digital preservation gives direction to the digital preservation policy, as to how everything stated in the policy can be achieved. A policy is not complete unless it has the support of a strategy.

Expressing the significance of a strategy, Dollar and Ashley (2015) proffer that a digital preservation strategy is one of the most important tools in the management of electronic records. According to Shimray and Ramaiah (2018), the strategy should aim to instruct users to convert their records to “preservation ready” formats before submitting them. Also, it must call for the monitoring of any changes in technology that may affect the preservation of electronic records.

As a result, changes in technology were not formally addressed at the OPM. Even though IT monitored and kept updating the EDRMS, they did it under no formal strategy. Explaining how the digital preservation strategy relates to the Policy, Shimray and Ramaiah (2018) state that, a Digital Preservation Strategy cannot exist in the absence of a policy.

Whilst the policy gives details why the chosen electronic records need to be preserved, the strategy states how it will be implemented.

5.2.2 Lack of governance frameworks

This study found out that the OPM did not have a formal information governance to assign accountability and authority for digital preservation. Howard (2013) stipulates that in the absence of a proper governance framework, most if not all aspects of governance, inclusive of accountability and authority, are compromised. Smallwood (2013) asserts that accountability and authority are vital in identifying those that should be involved in digital preservation, both within and outside the archive and their roles. Their roles should be made clear and distinctive to ensure that they understand their authority and that they could be held accountable for their actions depending on their roles.

Equally important, in the management of records, a governance framework should exist to ensure compliance of the preservation repository with applicable laws and regulations, the records retention schedule, and the disposition authorities and standards (Dollar & Ashley, 2015).

Franks (2020) reports that in every setting, order can only be ensured if there is a legal framework with guidelines on what is allowed to be done and what is not. In records management, a governance framework allows for institutions to adhere to what is allowed to be done and avoid what is not allowed to be done.

According to Brooks (2019), in the absence of a governance framework, records management would probably differ from one institution to the other. There would be no uniformity in terms of how records are managed, because the management of records is not controlled and regulated by any framework.

Therefore, a governance framework creates uniformity in records management. It is ideal that the organisation adopts an enterprise digital preservation governance framework, inclusive of policies and procedures to support the repository or repositories. Because of the possible changes in technology and other requirements, the framework must be reviewed at least after every two years (Smallwood, 2013; Dollar & Ashley, 2015).

Smallwood (2013) warns that every organisation in the business of digital preservation must have a governance framework specifically for electronic records management. Furthermore, the governance framework should ensure compliance with all applicable laws and adherence to both local and international standards.

5.2.3 Lack of collaboration

The results of this study show that the OPM did not have any framework to allow it to collaborate with standing partners. Altman et al. (2009) state that Digital Preservation is too complex to successfully and effectively pull off as a single organisation without having to collaborate with stakeholders or other entities in the same line of business.

Dollar and Ashley (2015) assert that it requires a lot of different resources, technologies and expertise to achieve and run an effective Digital Preservation programme. Organisations in the business of Digital Preservation should therefore venture into collaborations with peer organisations, not only for the purpose of sharing resources, but also to share information on latest technologies and be up to date with the best systems as well as records management best practices (Pinnick, 2017).

According to Dollar and Ashley (2015), a collaboration framework should not necessarily be about technical expertise, but it should see the organisation reaching out to its stakeholders to identify and eventually meet the requirements of digital preservation.

Altman et al. (2009) further stipulate that many stakeholders are involved in digital preservation and they all play vital roles in the process, from IT, software developers and other support functions. It is thus important that the organisation's collaboration realises the relationship between and within all its stakeholders because they depend on each other.

5.2.4 Lack of training and limited technical expertise

According to the findings of this study, the OPM had qualified personnel for positions involving electronic records management. Dollar and Ashley (2015), report that Digital Preservation involves advanced technologies and systems which may require advanced levels of expertise in different fields and departments.

It is thus highly recommended that institutions trusted with the long-term preservation of electronic records have sufficient and qualified personnel in all positions involving electronic records management (Blumenthal et al., 2020).

Results of this study further revealed that apart from their qualifications and academic expertise, their employees did not receive any further training with regards to Digital Preservation. Furthermore, there were no measures in place to make sure that the employees were equipped and up to date with relevant and necessary expertise. In addition, the OPM did not have any internal or external operational access to specialised professional and technical expertise in digital preservation or electronic records management.

Technology is advancing very fast that staff members will require extra training in different areas of their jobs. It is important that they have access to either internal technical expertise, if the organisation has the capacity, or external (Penn & Pennix, 2017).

Access to technical expertise, either internally or from outside is vital throughout the entire process of digital preservation. For instance, from ingestion, users or producers must have expertise assistance to help them with changing their records into preservation ready formats. This expertise would also come in handy when the repository needs to examine the potential impacts of emerging technologies on digital preservation (Dollar et a., 2014).

Pinnick (2017) argues that whilst having qualified employees is vital, with changes in technology, it is advisable to make sure that employees are up to date with knowledge of the latest systems, technologies and practices. Employers should therefore organise appropriate training for their staff. Equally important, they should also have access specialised professional and technical expertise, either within the organisation or externally.

5.2.5 Poor engagement with the designated community and insufficient electronic records survey

Even though the EDRMS was implemented to cater for the entire Namibian public sector, this study established that the OPM did not have any written agreements with users and producers in terms of rights, obligations and responsibilities as far as transfer, custody and dissemination are concerned. Basically, there was no formal document defining the rights, obligations and responsibilities of the designated community for electronic records to be transferred to the repository.

Digital preservation exists with many stakeholders and requires that all stakeholders are effectively engaged and they are made aware of their roles and responsibilities in the entire process of digital preservation (Saini, 2018).

This implies that the repository barely engages the designated community. The organisation should engage users and producers of records within their organisation, not only to establish agreements about rights and responsibilities for transferring records to the repository, but also to take note of their evolving needs and requirements in terms of digital preservation (Dollar & Ashley, 2015; ISO, 2012).

As far as this study is concerned, the OPM had, at least once, carried out an Electronic Records Survey. Its main aim was to verify if different departments, ministries and other government institutions had the required infrastructure before implementing the EDRMS.

Altman et al. (2009) recommend that the electronic records survey should identify the volumes of records which merit long-term preservation and categorise all preservation ready, near-preservation ready, and legacy permanent electronic records. These may include emails and other electronic correspondences.

Normally, a records survey is an organised action aimed at locating and identifying all the records held by a certain institution. However, there is more to Electronic Records Survey than just locating and identifying records. In digital preservation, the survey includes identifying the media format, type and size (Altman et al., 2009). Idrissi (2019) affirms that Electronic Records Survey is normally done to help in the collection of information about electronic records as both the creator and the repository prepare for transfer.

5.3 Adherence of the preservation repository to the accepted operational practices

Under this objective, the researcher was able to assess the conformance of the EDRMS to the accepted operational practices of electronic records management and digital preservation. The study findings in this regard are discussed and interpreted according to the following sub-headings:

- Open Standards Technology Neutral Formats and media renewal
- Integrity and security
- Preservation metadata and archival storage

5.3.1 Open Standards Technology Neutral Formats and media renewal

It was established that the OPM adopted PDF as their preferred format.

According to Smallwood (2013), preservation repositories must make use of Open Standards Technology Neutral Formats because these types of formats do not normally depend on technology.

It is further advised that creators of records should submit their records in preservation-ready formats, especially for records which merit long term preservation.

However, the OPM did not have a technology watch programme in place, to monitor the sustainability of this format. Idrissi (2019) asserts that the mitigation of file format obsolescence involves supporting a watch programme on the sustainability of file formats.

Equally important, it was discovered that PDF was the only format adopted by the OPM as a preferred digital preservation format. However, ISO (2003) recommends that the repository adopts as many open standard technology neutral formats as preferred digital preservation formats, as possible. It was further advised that the repository keeps monitoring and identifying any other new OS/TN formats before adopting them as suitable to be used as preferred formats.

Dollar and Ashley (2015) describe an effective media or device renewal programme as the one that always keeps inspecting for possible loss of readability of the electronic records and replaces the media automatically. Nonetheless, the findings of this study have revealed that the OPM repository did not have any media renewal protocol. In addition, the system could not automatically monitor the potential loss of readability.

Given the fact that all storage media can go obsolete, it may seem that the only way for repositories trusted with long term preservation, keep monitoring the readability of their storage media or devices.

It is therefore recommended that a trustworthy repository should have in place a protocol for constantly monitoring the readability of devices (Abrams, 2005).

5.3.2 Integrity and security

As per the findings of this study, the repository at the OPM did not have a documented procedure for integrity protection of electronic records.

Most authors have however, warned against this type of practice. Digital preservation is a complex process. During this process, records go through different phases, some of which may cause harm or loss of physical and intellectual information. Institutions mandated to preserve long-term and permanent electronic records must therefore have mechanisms in place to ensure the integrity of records in their custody (ISO, 2003; Idrissi, 2019).

The EDRMS could however produce an audit trail which can be used to detect any changes in records. Idrissi (2019) states that the best way to monitor the integrity of electronic records is through an automated system, which would automatically identify any change that may have happened during all the processes of digital preservation.

Even though the OPM did not have a written preparedness and recovery plan specifically for electronic records, records on the system were backed up and there was an offsite storage in case of emergencies. However, Ngulube and Adu (2016) report that having in place a written disaster preparedness and recovery plan in place is necessary as it aids in reducing risks and decreases liability. It would mean that required data would remain accessible in the event of disaster, because this ensures a continuous flow of information across the organisation.

The study has also established that access to the EDRMS at the OPM is password-protected. Unlike paper records which are secured by physical locks, electronic records are preserved in systems, and if no appropriate security measures are in place, anyone with a computer could possibly access them. It is therefore recommended that access be regulated to allow access to authorised personnel only (Dollar & Ashley, 2015).

Unlike locking a physical room, securing a system from unauthorised access is much more complicated. Even if the system is password protected, there are hackers who, with help of sophisticated software could bypass security and enter the system. Therefore, it is advisable to have strong firewalls to defend the system against potential hackers (Kruse et al., 2017).

The server room was also fitted with appropriate security measures as per the ISO requirements. The server room acts as the actual preservation repository because that is where the actual equipment and technologies which run the system are. It is warned that the server room is protected at all time and entry should be regulated. In case of unusual visitors, details should be taken and their movements monitored (Yang & Li, 2018). Apart from outsiders, staff members who have access to the server room must also be trusted. A staff member is equally a threat to the server room. It is advised that CCTV cameras are working and reviewed regularly, just to make sure that nothing fishy goes on in the server room (Griffith, 2019).

In spite of all the security measures surrounding the EDRMS, the OPM did not have any formal mechanism to regularly monitor security protection processes. It is recommended that security protection processes must be regularly monitored and revised due to the ever-changing technologies and business needs (Dollar & Ashley, 2015).

5.3.3 Preservation of metadata and archival storage

This study found out that the EDRMS allowed metadata to be captured manually and separately and that records could not be uploaded to the system without complete metadata. Metadata determines the integrity of a record. Unless a record is captured with its full metadata, complete and unaltered, such a record has no integrity and cannot be considered reliable (Dappert & Enders, 2010).

The EDRMS could also automatically produce an audit trail to show any change that may have been made to the metadata. Dollar and Ashley (2015) dictate that preservation repositories must have appropriate measures in place to make sure that AIPs are complete. Dappert and Enders (2010) affirm that the system must be able to automatically detect any changes in the metadata of a record throughout the entire preservation process and assure that they remain intact.

This study affirmed that the OPM repository did not consist of any primitive archival storage.

Digital preservation repositories should at all costs avoid archival storage media which are primitive. Every media is prone to deterioration, but some are too sensitive and they can be easily ruined (Idrissi, 2019).

It was also discovered that the repository had two geographically separated instances of the preservation repository. It is advised that an institution trusted with long term preservation of electronic records must have more than one instance of the preservation repository which supports the storage of AIPs and they should be geographically separated (ISO, 2003).

An ultimate archival storage should consist of at least two instances of preservation repository capable of storing AIPs. These instances should not be in the same geographical location.

Equally important, the completeness of records should be verified automatically. This information should then be transferred to PDIs, to form an auditable chain of electronic custody (Idrissi, 2019).

5.4 Safety of electronic records when undertaking business actions

This objective aimed at establishing the extent to which the OPM ensures the well-being of electronic records throughout all the processes and activities of digital preservation services. The following sub headings were a result of the findings.

- Ingest
- Access

5.4.1 Ingest

This study discovered that during ingestion, the OPM did not have any agreements with producers with regards to format, integrity, virus checks, metadata checks and quality.

However, the system could detect any incomplete metadata during the process of uploading. Ingestion is a stage that should include efforts from both the producers and the repository.

The repository plays a bigger role of making sure that there are agreements between them and the producers in terms of the formats of records being deposited, integrity, virus checks, metadata and quality (Smallwood, 2013).

Producers on the other hand should make sure that they adhere to the terms and conditions as per all the agreements with the repository. Ruusalepp and Dobreva (2015) state that it is important that these agreements are adhered to. In case something goes wrong, the two parties will know who to hold accountable.

Dollar and Ashley (2015), allege that the most effective way is to make sure that SIPs are ingested automatically, and the system automatically verifies the completeness of metadata in terms of administration, technical, provenance, content description, and preservation description of significant properties. These properties must then be copied from the SIPs to Preservation Description Information (PDI), which are then transferred to the repository for storage.

5.4.2 Access

Findings of this study have established that the EDRMS allowed users and producers access to their records in the comfort of their own offices through an integrated search functionality. Dollar and Ashley (2015) urge that institutions in the business of preserving electronic records should be able to not only make sure that such records remain accessible for as long as they are needed, but also allow users access in the most appropriate and easiest platforms possible. In addition, it is important to make sure that all records in digital format remain readable with recent technology. It is of no use to have information available, but cannot be read or interpreted with recent technology (Matusiak et al., 2017).

Access must be allowed in the form of Dissemination Information Packages (DIP), which should be produced automatically through an integrated search functionality. Information searched for by users could be used to audit the production of DIPs (Dollar & Ashley, 2015; ISO, 2012).

5.5 Chapter summary

This chapter interpreted and discussed the findings of the study as discovered. The interpretation and discussion of findings was arranged into themes which came about as a result of the data in an attempt to satisfy all the objectives of this study. Firstly, this chapter presented findings on the commitment of the OPM, sustainability and the adequacy of its resources.

It was discovered that even though the EDRMS was introduced over ten years ago, it has been operational in the absence of a digital preservation policy. Equally important, the OPM did not have any formal strategy in place to address possible changes in technology. Moreover, the OPM lacked most of the relevant governance frameworks, including a formal information governance to assign accountability and authority for digital preservation. This study also discovered that the OPM did not have a framework to allow it to collaborate with standing partners and other stakeholders. Even though the OPM had qualified personnel in all areas surrounding records management, these staff members have never received any further training in terms of electronic records management. Furthermore, staff members also do not have any access to any specialised professional and technical expertise. As a result, their skills and capabilities are only limited to their qualifications, most of which are not even specialised to electronic records management. It could also be established that the engagement of the registry with its stakeholders was poor such that there were no agreements in place with users and producers in terms of rights and obligations as well as the dissemination of information. The records survey which was done did not capture the entire information required for the implementation of a digital preservation programme.

The chapter then presented and interpreted the findings on the adherence of the Preservation Repository to the accepted operational practices. It was discovered that the OPM adopted PDF as the only preferred digital preservation format.

There was, however, no technology watch programme to monitor the sustainability of such a format. In addition, the repository did not have a documented procedure for integrity protection of electronic records, but the system could produce an audit trail of the movement of records and detect any possible changes made. Equally important, there was no written preparedness and recovery plan specifically for electronic records, but IT had a backup of the information.

The system captures metadata manually and the repository does not consist of any primitive archival storage. Finally, findings on the safety of electronic records throughout all business actions were presented. It was established that even though the system could detect any incomplete metadata during ingestion, the repository did not have agreements with producers with regards to format, integrity, virus checks, metadata checks and quality. Moreover, the system allowed users and producers access to their records through an integrated search functionality. The next chapter presents a summary of the findings of the study, conclusions and recommendations.

CHAPTER SIX

SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter summarises the research findings presented and interpreted in the two previous chapters (chapters four and five), according to the objectives of the study. Furthermore, the chapter makes conclusions and shows how all the objectives of the study were satisfied. Equally important, the chapter presents how this study contributes to the already existing body of knowledge on digital preservation, specifically digital preservation maturity. Moreover, the chapter presents recommendations on how the DPCMM model can be used by institutions in the business of long-term preservation of electronic records, to assess the effectiveness of their digital preservation programmes and subsequently create a road map for an improved digital preservation environment. Finally, the chapter presents possible areas for further research in terms of digital preservation as unveiled by this study.

6.2 Conclusions

Under this subsection, conclusions and a final analysis of the establishments of this study are made according to the three objectives of this study. Conclusions of the fourth objective of the study, which is to determine the roles of users and producers in the process of digital preservation, is done under the other three objectives. This subsection also explains how these objectives were fulfilled. The main objective of the study was to assess the digital preservation of the OPM of Namibia. In that regard, the main objective was categorised into the following objectives:

6.2.1 The commitment of the OPM as well as the sustainability and adequacy of its resources in ensuring effective digital preservation

According to the findings of this study, there was no digital preservation policy. Furthermore, there was no digital preservation or electronic records management strategy in place. Moreover, there was no formal document detailing how the EDRMS programme would be supported. Equally important, changes in technology were not formally addressed. However, IT kept updating the system even in the absence of a formal strategy. The OPM also lacked some important governance frameworks. One such framework is the formal information governance to assign accountability and authority for digital preservation. In addition, there was no distinctive and clear role of different stakeholders on digital preservation.

Moreover, there was no formal governance framework to ensure compliance of the preservation repository with applicable laws, regulations, records, retention schedule, disposition authorities and standards. In this regard, the study concludes that the EDRMS was implemented in the absence of very crucial tools and guidelines of digital preservation.

It is further concluded that the absence of a digital preservation policy compromises some other important tools like the digital preservation strategy, as well as electronic records management guidelines. This study also concludes that the roles of users, producers and other stakeholders are not distinctive and clear enough, as there is no document which clearly details issues of authority and responsibility.

In addition, the OPM may not be in full conformance to some laws, as far as the management of electronic records is concerned. This is because they do not have a formal governance framework to ensure compliance of the preservation repository with applicable laws.

The study further established that there was no framework to allow the OPM to collaborate with standing parts.

Moreover, there were qualified personnel in all areas of records management, but staff members involved in the electronic records management had not received any further training in terms of digital preservation. In addition, they did not have any external operational access to specialised professional expertise. Staff members would, however, technically help each other within the organisation. Also, the repository did not have any written agreements with users and producers of records in terms of rights, obligations and responsibilities as far as transfer, custody and dissemination are concerned. Therefore, this study has concluded that the OPM was not in any collaboration with any peer organisation, as far as digital preservation is concerned. The only collaboration they had was within the organisation, whereby different departments of the organisation work hand in hand.

It is also concluded that the repository lacked formal engagement with users. The rights, obligations and responsibilities of users and producers are clear as they do not have any agreements with the repository in that regard.

6.2.2 Adherence of the preservation repository to the accepted operational practices

It is established that the OPM adopted PDF as their only preferred digital preservation format. However, there was no formal technology watch programme in place to monitor

the sustainability of this format. Furthermore, there was no media renewal protocol to renew possible outdated media. The IT personnel however, keep updating the system on their own terms. Equally important, the repository did not have a documented procedure for integrity protection of electronic records. The EDRMS could, however, produce an audit trail which can be used to detect any changes in records. Moreover, the OPM did not have a written disaster preparedness and recovery plan specifically for electronic records. However, records on the system were backed up and there was an offsite storage in case of emergencies.

Access to the EDRMS was protected by way of passwords. The server room was also fitted with appropriate security measures as per the ISO requirements. In spite of all the security measures surrounding the EDRMS, the OPM did not have any formal mechanism to regularly monitor security protection processes. It was found that the EDRMS allows metadata to be captured manually and separately and records could not be uploaded to the system without complete metadata. The repository did not consist of any primitive archival storages. In addition, they had two geographically separated instances of the preservation repository. It is, therefore concluded that the OPM repository only had one format that had been adopted as a preferred digital preservation format.

Even though there are some security measures in place, the repository did not have a written disaster preparedness and recovery plan and their security protection processes were not monitored, regularly. It can also be concluded that metadata of records were captured entirely and users could access their records by searching using a keyword on the system.

6.2.3 Safety of electronic records when undertaking business actions

It was discovered that during the ingestion process, the repository did not have any agreements with producers with regards to format, integrity, virus checks, metadata checks and quality. However, the system could detect any incomplete metadata during the process of uploading. Furthermore, users were allowed access to records through an integrated search functionality. Therefore, this study concludes that there was a lack of awareness for users in terms of what was expected of them during ingestion. This is because there were no agreements with the repository or guidelines to indicate to them what was expected of them in terms of ensuring the integrity of their records.

It is also concluded that viruses could be a matter of concern as there were no mandatory virus checks during ingestion. This study also concludes that access to records was allowed through an integrated search functionality of the EDRMS.

6.3 Recommendations

The following are recommendations which emanate from the findings of this study. They are presented according to the findings of the study.

6.3.1 The commitment of the OPM as well as sustainability and adequacy of its resources in ensuring effective digital preservation

- In the absence of a policy, the OPM should consider drafting and implementing a policy which can cater specifically for the management of electronic records.

- The policy should include a formal strategy to monitor any possible changes in technology; a formal information governance to assign accountability and authority for digital preservation and a governance framework to ensure compliance of the preservation repository with applicable laws, regulations, a records retention schedule, disposition authorities and standards.

  The National Archives of Namibia seems to be the appropriate institution for the implementation of such a policy. They could benchmark with other organisations and institutions in the same business.
- The OPM currently do not have a governance framework. Therefore, they need to have a proper and formal information governance framework. Such a framework should assign accountability and authority for the preservation of electronic records by clearly identifying stakeholders involved and their roles, distinctively.

  In addition, the governance framework should ensure compliance of the preservation repository with applicable laws and regulations, the records retention schedule, disposition authorities and standards.
- Currently, the OPM does not collaborate with any standing partners. Therefore, they should invest in collaborating with standing partners, peer organisations and all stakeholders, not only in the public service, but private organisations with the same mandate as well. Digital preservation is a broad discipline and it requires advanced technology and expertise. An individual organisation would have a hard time pulling off a successful digital preservation programme all by itself, hence the importance of collaboration.

Having in place a collaboration framework would allow the OPM to successfully engage its stakeholders on identifying and meeting digital preservation requirements. Adequate and appropriate training as well as access to specialised professional technical expertise can also come in handy.

- OPM employees do not have access to specialised professional technical expertise, or offer them additional training. Even with qualified employees, the OPM should make provisions for additional training, at least for employees dealing with electronic records management. Training should focus on, among others, the use of recent technologies, software and records management best practices. In addition, the OPM should also provide these employees access to specialised professional technical expertise either within the organisation or externally, in areas related to digital preservation.

6.3.2 Adherence of the preservation repository to the accepted operational practices

- Because the OPM have identified only one format as their preferred format, the study recommends that the OPM starts to monitor, identify and eventually adopt as many formats as preferred digital preservation formats.

  The PDF may seem sufficient now that they are using EDRMS just to scan and upload, which is not entirely sufficient. Once they start conducting business processes electronically, there will be a need for additional formats. There should also be a formal technology watch programme to monitor the sustainability of those formats to mitigate file format obsolescence.

- In terms of security and integrity, the OPM has a lot to do. They should start by drafting and implementing a disaster preparedness and recovery plan for the management of electronic records. The right institution to do this would be the National Archives of Namibia. In addition, the EDRMS should be able to automatically detect any changes or alterations that are made to the records throughout the process of digital preservation. It should also be able to automatically capture metadata. Due to the ever-changing nature of technology, they should also monitor and revise their security protection processes.

6.3.3 Safety of electronic records when undertaking business actions

- The OPM currently do not have any signed agreements with users. It is recommended that the repository has written agreements with the users of the system before they can actually use the system. Therefore, the OPM needs to come up with some agreements. The agreements must be regarding format, integrity, virus checks, metadata checks and quality. As it stands, users can upload anything in PDF format regardless of the quality or virus status. The ingestion process must therefore be regulated.

6.4 Contribution to the body of knowledge

In academia, this study contributes to the existing body of knowledge in terms of digital preservation, by filling the gap in literature around digital preservation, particularly digital preservation maturity. As far as this researcher is concerned, no study in Namibia, before this one, had focused on the assessment of digital preservation maturity. However, different researchers have conducted their studies in the context of their respective countries and Africa at large.

Some have reported on the digitisation maturity of Africa as a continent, concluding with shortcomings, challenges and recommendations (Siemens, 2017). Some have tackled digital transformation in different industries of their countries (Ezeokoli et al., 2016), while others have researched on what is required to reach a better digital maturity level (Kane et al., 2017). In Namibia on the other hand, most researchers in the area of digital preservation have based their studies on digital preservation in general. Some investigated the preservation of audio-visual records (Iipinge & Mnjama, 2017), and preservation of electronic records (Nengomasha, 2009), while others tackled the development of a digitisation programme (Hillebrecht, 2011). Therefore, in terms of assessing the digital preservation and electronic records management programme, the present research is a pioneer study, especially in the Namibian context.

Practically, this study contributed to the body of knowledge through investigating and assessing the digital preservation of the EDRMS of the OPM. Results and recommendations generated by this study would, therefore, not only add to the existing knowledge about digital preservation, but, it will also be useful, not only to the OPM and the Namibian public sector, but to any other institutions, mandated to preserve electronic records which merit long-term preservation.

6.5 Areas for further research

This study focused on assessing the maturity of the Electronic Document Records Management System (EDRMS) programme at the OPM. The study suggests the following for future investigation and further research:

a) Assessing the impact of the implementation of the EDRMS on service delivery within the public sector;

b) Investigating the role of collaboration and its impact on the effectiveness of digital preservation; and
c) Investigating the importance of training and technical expertise on the success of the electronic records management programme.

6.6 Final conclusion

This study sought to assess the commitment of the OPM as well as the sustainability and adequacy of its resources in ensuring effective digital preservation; to establish the extent to which their repository and preservation environment adheres to the accepted operational practices of ISO 14721 and ISO 16363 respectively; to establish the extent to which the integrity, security, usability and accessibility of digital records is assured when undertaking business actions; and to determine the roles of producers and users from creation to transfer as well as the use of digital records. This qualitative study made use of semi-structured interviews and observation as data collecting methods, and these were supplemented by documents review.

All employees of the OPM constituted the population of the study. The study made use of non-probability sampling techniques, specifically the purposive and snowball sampling techniques.

The data collected by this qualitative study were analysed through the use of content analysis and presented through descriptive narratives in which tables and diagrams were also used. Findings were discussed in subheadings: Digital Preservation Policy; Digital Preservation Strategy; Governance; Collaboration; Technical Expertise; Designated Community; Electronic records survey; Open Standard Technology Neutral Formats; Media/Device renewal; Integrity; Security; Preservation metadata; Archival storage;

Ingest; Access, as well as Producers and Users. This chapter also made a summary of the study findings which were arranged according to the same sub headings as the discussion of findings.

Not every digital preservation programme is effective. The effectiveness of a digital preservation programme is not determined sorely by the ability to preserve digital information, but it should also be able to provide access to trustworthy digital records for as long as they are needed. An effective digital preservation programme should also fully conform to all records management standards and good practices. This study has proven that the assessment of a digital preservation programme does not only reveal how effective the programme is, but it also highlights different areas within the programme which may need improving. Therefore, it is of utmost importance that digital preservation programmes are assessed.

REFERENCES

Ab Aziz, A., Mohammad Yusof, Z., Mokhtar, U. A., & Jambari, D. I. (2018, March). *Electronic document and records management system implementation in Malaysia: A preliminary study of issues embracing the initiative.* https://www.researchgate.net/profile/Azlina-Aziz/publication/327198981_A_Conceptual_Model_for_Electronic_Document_and_Records_Management_System_Adoption_in_Malaysian_Public_Sector/links/5bc5948aa6fdcc03c788f573/A-Conceptual-Model-for-Electronic-Document-and-Records-Management-System-Adoption-in-Malaysian-Public-Sector.pdf

Abrams, S. L. (2005). Digital formats and preservation. https://ipres-conference.org/ipres05/download/Digital%20Formats%20And%20Preservation%20-%20Stephen%20Abrams.pdf

Adhabi, E., & Anozie, C. B. (2017). Literature review for the type of interview in qualitative research. *International Journal of Education*, *9*(3), 86-97. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_vis=1&q=interview+qualitative+data+collection+methods&btnG=

Al-Ababneh, M. M. (2020). Linking ontology, epistemology and research methodology. *Science & Philosophy*, *8*(1), 75-91. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3708935

Altman, M., Adams, M., Crabtree, J., Donakowski, D., Maynard, M., Pienta, A., & Young, C. (2009). Digital preservation through archival collaboration: The data preservation alliance for social sciences. *The American Archivist, 72*(1), 170-184. https://doi.org/10.17723/aarc.72.1.eu7252lhnrp7h188

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. https://journals.sagepub.com/doi/full/10.1177/1609406919874596

Arifin, M. S. R. (2018). Ethical consideration in qualitative study. *International journal of care scholars, 2*(1), 30-33. https://journals.iium.edu.my/

Ashenfelder, M. (2017). Developing a digital preservation infrastructure at Georgetown University Library. https://blogs.loc.gov/thesignal/2017/03/developing-a-digital-preservation-infrastructure-at-georgetown-university-library/

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Nursing plus open, 2*(1), 8-14. https://www.sciencedirect.com/science/article/

Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses Association*, *22*(2), 27-30. https://search.informit.org/doi/abs/10.3316/INFORMIT.738299924514584

Blumenthal, K. R., Griesinger, P., Kim, J. Y., Peltzman, S., & Steeves, V. (2020). What's wrong with digital stewardship: evaluating the organization of digital preservation programs from practitioners' perspectives. *Journal of Contemporary Archival Studies, 7*(1), 13. https://elischolar.library.yale.edu/jcas/vol7/iss1/13/

Brooks, J. (2019). Perspectives on the relationship between records management and information governance. https://www.emerald.com/insight/content/doi/10.1108/RMJ-11-2016-0042/full/html

Brown, A. (2013). *Practical digital preservation: A how-to guide for organizations of any size.* Facet publishing.

Bulow, A. E., & Ahmon, J. (2011). *Preparing collections for digitization*. Facet Publishing.

Bunawan, A. A., & Nordin, S. (2015). The challenges in preserving the electronic records metadata. *Int J Information Syst Eng*, *1*(1), 1-7. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0312986f4616784638775d0920c2b12e985d9d34

Connelly, L. M. (2014). Ethical consideration in research studies. *Medsurg Nursing*, *23*, 1-54. https://link.gale.com/apps/doc/

Corrado, E. M. (2019). Repositories, trust, and the coretrustseal. *Technical Services Quarterly*, *36*(1), 61-72. https://www.tandfonline.com/doi/abs/10.1080/07317131.2018.1532055

Da Silver, J. L., & Borges, M. M. (2017). Digital preservation policies of the institutional repositories at Brazilian Federal Universities. *The Electronic Library, 35*(2), 311-321. https://doi.org/10.1108/EL-09-2015-0170

Dappert, A., & Enders, M. (2010). Digital preservation metadata standards. *Information Standard Quarterly, 22*, 2-31. https://www.loc.gov/standards/premis/FE_Dappert_Enders_MetadataStds_isqv22no2.pdf

Dollar, C. M., & Ashley, J. L. (2015). *Digital preservation maturity model*. https://static1.squarespace.com/.../dpcmm+background+and+performance+metrics

Dollar, C. M., Ashley, J. L., & Misic, M. (2014). *Building the business case for digital preservation using the digital preservation capability maturity model*. http://brtf.sdsc.edu/biblio/BRTF_Final_Report.pdf.

Donaldson, D. R. (2020). Certification information on trustworthy digital repository websites: A content analysis. *Plos one*, *15*(12). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0242525

Drisko, J.W., & Maschi, T. (2016). *Content analysis: Pocket guide to social work research methods*. Oxford University Press. https://books.google.com.na/books?id=07GYCgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Dryden, J. (2011). Measuring trust: Standards for trusted digital repositories. *Journal of Archival Organizations, 9*(2), 127-130. https://doi.org/10.1080/15332748.2011.590744

Dudovskiy, J. (2009). *The ultimate guide to writing a dissertation in business studies: A step by step assistance*. https://www.bcps.org/offices/lis/researchcourse/.com

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, 7(3), 93-99. https://www.sciencedirect.com/science/article/pii/S2211419X17300423

Ezeokoli, F. O., Okolie, k., C., Okoye, U., P., & Belonwu, C., C. (2016). Digital transformation in the Nigeria construction industry: The professionals' law. *World Journal of Computer Application and Technology*, *4*(3) 23-30. Doi:10.13189/wjcat.2016.040301

Frank, R. D. (2022). Risk in trustworthy digital repository audit and certification. *Archival Science, 22*(1), 43-73. https://link.springer.com/article/10.1007/s10502-021-09366-z

Franks, P. C. (2020). Implications of blockchain distributed ledger technology for records management and information governance programs. *Records Management Journal, 30*(3), 287-299. https://www.emerald.com/insight/content/doi/10.1108/RMJ-08-2019-0047/full/html

Gallinger, M. (2021). *History of the DPCMM*. https://www.statearchivists.org/blogs/michelle-gallinger/2021/10/19/2022-dpcmm-history-of-the-dpcmm

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal, 204*, 291-295. https://doi.org/10.1038/bdj.2008.192

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8*(4), 597-607. http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Grant, C., & Osanloo, A. (2014). Understanding, selecting and integrating a theoretical framework in dissertation research: Creating the blueprint for your house. *Administrative Issue Journal, 4,* 2, 12-26. https://files.eric.ed.gov/fulltext/EJ1058505.pdf

Greetman, B. (2009). *How to write your undergraduate dissertation*. Palgrave Macmillan.

Griffith, R. (2019). Electronic records, confidentiality and data security: the nurse's responsibility. *British Journal of Nursing, 28*(5), 313-314. https://www.magonlinelibrary.com/doi/abs/10.12968/bjon.2019.28.5.313?journalCode=bjon

Grimm, S. (2016). *Practical digital preservation 2016/2017.* https://www.statearchivists.org/files/1714/8589/3400/Protecting_and_Preserving_Long-Term_Digital_Information_COSA_Jan17_v07.pdf.

Hillebrecht, W. (2011). *Establishing a digitization programme for Namibia: Promise, pitfalls and progress.* http://hdl.handle.net/10539/11504

Howard, I. (2013). *Information governance: A brief introduction - New Zealand focus*. https://www.researchgate.net/publication/264742401_Information_Governance_A_Brief_Introduction_-_New_Zealand_Focus

Hughes, L. M. (2014). *Digitizing collections: Strategic issues for the information manager*. Facet Publishing.

Idrissi, B. (2019). *Long-term digital preservation: A preliminary study on software and format obsolescence.* https://www.researchgate.net/publication/335083900_Long-Term_Digital_Preservation_A_Preliminary_Study_on_Software_and_Format_Obsolescence

Iipinge, H. L., & Mnjama, N. (2017). Preservation of audio-visual records at the National Archives of Namibia. *Journal of the South African Society of Archivists*, 50, 79-99.

ISO (2003). *Space data and information transfer systems - Open Archival Information System-Reference Model*. https://www.sis.se/std-903580

ISO (2012). *Space data and information transfer system-Audit and certification of trustworthy digital repositories*. https://www.iso.org/standard/56510.html

Kane, G. C., Palmer, D., Phillips, A., N., Kiron, D., & Buckley, N. (2017). *Achieving digital maturity: Adapting your company to a changing world.* https://www.deloitte.com/content/dam/insights/us/articles/3678_achieving-digital-maturity/DUP_Achieving-digital-maturity.pdf

Kivunja, C. & Kuyini, A. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education, 6* (5), 26-41. https://doi.org/10.5430/ijhe.v6n5p26

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of medical systems, 41*, 1-9. https://link.springer.com/article/10.1007/s10916-017-0778-4

Mack, N., Woodsong, B., Macqueen, K. M., & Guest, G. (2005). *Qualitative research methods: A data collector's field guide.* https://course.ccs.neu.edu/is4800sp12/resources/qualmethods.pdf

Maemura, E., Moles, N., & Becker, C. (2017). Organisational assessment framework: A literature review and mapping. *Journal of the Association for Information Science and Technology*, *66*(7), 1619-1637. https://www.researchgate.net/profile/Christoph-Becker-7/publication/316573946_Organizational_assessment_frameworks_for_digital_preservation_A_literature_review_and_mapping/links/59c04724458515e9cfd5512d/Organizational-assessment-frameworks-for-digital-preservation-A-literature-review-and-mapping.pdf

Maree, J. G. K. (Ed.). (2013). *Complete your thesis or dissertation successfully: Practical guidelines* (5th ed.). Juta and Company ltd.

Masenya, T. M., & Ngulube, P. (2019). Digital preservation practices in academic libraries in South Africa in the wake of the digital revolution. *South African Journal of Information Management, 21*(1), 1-9. https://journals.co.za/doi/epdf/10.4102/sajim.v21i1.1011

Matusiak, K. K., Tyler, A., Newton, C., & Polepeddi, P. (2017). Finding access and digital preservation solutions for a digitized oral history project: A case study. *Digital library perspectives*, *33*(2), 88-99. https://www.emerald.com/insight/content/doi/10.1108/DLP-07-2016-0025/full/html

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach* (3rd ed.). SAGE Publications. https://books.google.com.na/books?id=xAHCOmtAZd0C&dq=qualitative+research+design&lr=&source=gbs_navlinks_s

Milian, E. Z., Spinola, M. D. M., & de Carvalho, M. M. (2019). Fintechs: A literature review and research agenda. *Electronic Commerce Research and Applications*, *34*. https://www.sciencedirect.com/science/article/abs/pii/S1567422319300109

Muray, N., & Hughes, G. (2008). *Writing up your university assignments and research projects: A practical handbook*. Open University press.

Murray, N., & Beglar, D. (2009). *Inside track: Writing dissertations and theses*. Pearson education limited.

Mwita, K. (2022). Factors to consider when choosing data collection methods. *International Journal of Research in Business and Social Science (2147-4478), 11*(5). https://www.ssbfnet.com/ojs/index.php/ijrbs/article/view/1842

Myers, J. L., Well, A., & Lorch, R. F. (2010). *Research design and statistical analysis*. Routledge. https://books.google.com.na/books?id=nbsOIJ_saUAC&dq=research+design&lr=&source=gbs_navlinks_s

Nengomasha, C. T. (2009). *Study of electronic records management in Namibia public service in context of e-government.* http://repository.unam.edu.na/handle/11070/447

Ngulube, P., & Adu, K. K. (2016). Key threats and challenges to the preservation of digital records of public institutions in Ghana. *Journal of Information Communication and Society, 20*(8), 1127-1145. https://doi.org/10.1080/1369118X.2016.1218527

Noble, H., & Smith, J. (2014). Qualitative data analysis: a practical example. *Evidence-Based Nursing, 17*(1), 2-3. https://ebn.bmj.com/content/17/1/2

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *BMJ Journals, 18*(2), 34-35. https://ebn.bmj.com/content/ebnurs/18/2/34.full.pdf

Noonan, D. W. (2014). *Digital preservation policy framework at the Ohio State University Libraries: A case study*. http://www.educause.edu/ero/article/digital-preservation-policy-framework-case-study

Note, M. (2019). Digital Archives: How and why to write digital preservation policy. https://lucidea.com/blog/how-and-why-to-write-digital-preservation-policy/

Nyampong, S. A. (2015). Electronic records management in national development: A case study in Ghana immigration services. *European Journal of Business Management, 10*(7), 120-145. https://core.ac.uk/download/pdf/234626429.pdf

OCLC. & CRL. (2007). *Trustworthy repositories audit and certification: Criteria and checklist*. http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

OPM (2009). *EDRMS for the public service: Project update*. https://www.opm.gov.na/documents/108506/160711/EDRMS.+Bulltein.pdf/00cfdc11-d65f-4f9e-950c-02d79aafb302

Paula, R., & Priest, H. (2006). Reliability and validity in research. *Nursing Standard, 20*(44), 41+. https://go.gale.com/ps/anonymous?id=GALE%7CA149022548&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00296570&p=HRCA&sw=w

Penn, I. A., & Pennix, G. B. (2017). *Records management handbook*. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9781315245140/records-management-handbook-ira-penn-gail-pennix

Pham, L. T. M. (2018). Qualitative approach to research a review of advantages and disadvantages of three paradigms: Positivism, interpretivism and critical inquiry. *University of Adelaide*. https://www.researchgate.net/publication/324486854_A_Review_of_key_paradigms_positivism_interpretivism_and_critical_inquiry

Pinnick, J. (2017). Exploring digital preservation requirements: A case study from the National Geoscience Data Centre. *Records Management Journal, 27*(2), 175-191. https://doi.org/10.1108/RMJ-04-2017-0009

Price, P. C., Jhangiani, R. S., & Chiang, I. C. A. (2015). Reliability and validity of measurement. *Research methods in psychology*. https://ecampusontario.pressbooks.pub/researchmethods/chapter/reliability-and-validity-of-measurement/

Rehman, A. A., & Alharthi, K. (2016). An introduction to research paradigms. *International Journal of Educational Investigations, 3*(8), 51-59. http://www.ijeionline.com/attachments/article/57/IJEI.Vol.3.No.8.05.pdf

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business research, 10*, 281-305. https://link.springer.com/article/10.1007/s40685-017-0045-z

Rieger, O. (2018). *The state of digital preservation in 2018: A snapshot of challenges and gaps.* https://sr.ithaka.org/wp-content/uploads/2018/10/SR-Issue-Brief-State-Digital-Preservation-20181022.pdf

Roller, M. R., & Lavrakas, P. J. (2015). *Applied qualitative research design: A total quality framework approach*. Guilford Publications. https://books.google.com.na/books?id=0zAXBgAAQBAJ&dq=qualitative+research+design&lr=&source=gbs_navlinks_s

Rosa, C. A., Craveiro, O., & Domingues, P. (2017). Open source software or digital preservation repositories: A survey. *International Journal of Computer Science and Engineering*, *8*(3), 21-39. https://www.researchgate.net/publication/318342833_Open_Source_Software_for_Digital_Preservation_Repositories_A_Survey

Ruusalepp, R., & Dobreva, M. (2015). *Digital preservation services: State of the art analysis.* https://tise2015.kku.ac.th/drupal/sites/default/files/Preservation_Services_study.Final_version.pdf

Saini, O. P. (2018). Understanding the role of institutional repository in digital preservation in academic libraries: A review of literature. *Library Philosophy and Practice*, *7*(2), 1-14. https://core.ac.uk/download/pdf/188140262.pdf

Shimray, S. R., & Ramaiah, C. K. (2018). *Digital preservation strategies: An overview*. https://www.researchgate.net/publication/327221006_Digital_Preservation_Strategies_An_Overview

Siemens. (2017). *African digitalization report 2017*. https://www.siemes.co.za/pool/about_us/digital_maturity_report_2017.pdf

Sittig, D. F., & Singh, H. (2012). Rights and responsibilities of users of electronic health records. *CMAJ, 184*(13), 1479-1483. https://www.cmaj.ca/content/184/13/1479.short

Smallwood, R. F. (2013). *Managing electronic records: Methods, best practices and technologies.* Wiley Publishers.

State of Michigan (n.d.). *Records management services: Frequently asked questions about electronic records for local governments*. https://www.michigan.gov/documents/hal_mhc_rms_electronic_records_125548_7.pdf

Stucky, H. L. (2015). The second step in data analysis: coding qualitative research data. *Journal of Social Health and Diabetes, 3*(1), 7-10. https://www.thieme-connect.com/products/ejournals/abstract/10.4103/2321-0656.140875

Thanh, N. C., & Thanh, T. T. (2015). The interconnection between interpretivist paradigm and qualitative methods in education. *American Journal of Educational Science, 2*, 1, 24-27. Retrieved from http://www.aiscience.org/journal/allissues/ajes.html

Thorne, S. (2000). Data analysis in qualitative research. *BMJ Journals, 3*(3), 68-70. https://ebn.bmj.com/content/ebnurs/3/3/68.full.pdf

UNESCO. (2021). *Concept of digital preservation*. https://en.unesco.org/themes/information-preservation/digital-heritage/concept-digital-preservation#:~:text=Digital%20preservation%20consists%20of%20the,hardware%20tools%20acting%20on%20data

University of Namibia (2013). *Research ethics policy, regulations and guidelines*. UNAM

Wilson, T. C. (2017). Rethinking digital preservation: definitions, models, and requirements. *Digital Library Perspectives*. https://www.emerald.com/insight/content/doi/10.1108/DLP-08-2016-0029/full/html

Yang, G., & Li, C. (2018, December). A design of blockchain-based architecture for the security of electronic health record (EHR) systems. https://ieeexplore.ieee.org/abstract/document/8591027

APPENDICES

Appendix A: Ethical Clearance Certificate

ETHICAL CLEARANCE CERTIFICATE

Ethical Clearance Reference Number: FOHM-012-2020 **Date: 09-09-2020**

This Ethical Clearance Certificate is issued by the University of Namibia Research Ethics Committee (UREC) in accordance with the University of Namibia's Research Ethics Policy and Guidelines. Ethical approval is given in respect of undertakings contained in the Research Project outlined below. This Certificate is issued on the recommendations of the ethical evaluation done by the Faculty/Centre/Campus Research & Publications Committee sitting with the Postgraduate Studies Committee.

Title of Project: ASSESSMENT OF DIGITAL PRESERVATION MATURITY (DPM) AT THE OFFICE OF THE PRIME MINISTER (OPM) OF NAMIBIA

Nature/Level of Project: HUMAN RESEARCH – NON-HEALTH: RESEARCH PROJECT

Researchers: ASSER LAUDIKA NAPANDULWE NAKALE

Student Nr: 201201492

Faculty: FACULTY OF HUMANITIES AND SOCIAL SCIENCES

Supervisors: PROF. T. KALUSOPA

Take note of the following:

(a) Any significant changes in the conditions or undertakings outlined in the approved Proposal must be communicated to the UREC. An application to make amendments may be necessary.

(b) Any breaches of ethical undertakings or practices that have an impact on ethical conduct of the research must be reported to the UREC.

(c) The Principal Researcher must report issues of ethical compliance to the UREC (through the Chairperson of the Faculty/Centre/Campus Research & Publications Committee) at the end of the Project or as may be requested by UREC. (d) The UREC retains the right to:

(i) Withdraw or amend this Ethical Clearance if any unethical practices (as outlined in the Research Ethics Policy) have been detected or suspected,

(ii) Request for an ethical compliance report at any point during the course of the research. REC wishes you the best in your research.

REC Chairperson

Dr R Bock

Appendix B: Request for permission to conduct research

Asser L N Nakale
P O BOX 24332, Windhoek
laudikanakale@gmail.com

0812878177

The Executive Director

Office of the Prime Minister

15 March 2021

RE: Request for permission to carry out a study

Dear Sir/Madam

I am a first-year student at the University of Namibia, studying towards a degree of **Masters in Records and Archives Management** (By Thesis). I am therefore required to carry out a study related to my field of study, hence writing this letter to request for permission to carry out research at your institution.

The study is titled**: "Assessing Digital Preservation Maturity (DPM) at the Office of the Prime Minister (OPM)"**. Being the leader of Government business in Parliament, with the mandate to coordinate the work of the cabinet as head of administration, the researcher believes that the OPM holds large volumes of digital records/Archives. It is within this background that this study seeks to assess the extent to which the OPM has gone as far as Digital preservation Maturity is concerned.

Being the first of its kind especially in Namibia as far as this researcher is concerned, this study would not only generate results that the OPM could use to develop strategies as well as a road map for incremental capability improvement, but it would also give recommendations according to the results. It would create awareness not only for the OPM, but other organisations involved in Digital Preservation on issues related to effective Digital Preservation.

I therefore request for your sincere consideration of this request. Detailed information is on the letter from my Supervisor, as well as a copy of my research proposal attached to this letter.

Should you require further information, do not hesitate to contact me on 081 287 8177.

I look forward to hearing from you soon.

Yours sincerely,

Asser L N Nakale (Student)

Appendix C: Research supervisor's support letter

University of Namibia, Private Bag 13301, Windhoek, Namibia
340 Mandume Ndemufayo Avenue, Pioneerspark
☎ +264 61 206 3111; URL.: http//www.unam.edu.na

UNAM
UNIVERSITY OF NAMIBIA

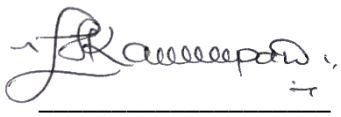
TO WHOM IT MAY CONCERN

This is to certify that **Mr. Asser Laudika Napandulwe Nakale** is a student at the University of Namibia pursuing a Masters of Arts in Records and Archives Management. Mr. Nakale has completed the proposal stage and should start with data collection as soon as possible. The topic the student is researching on is: ***'Assessment of Digital Preservation Maturity at the Office of the Prime Minister (OPM)'***. The main objective of this study is to assess the Digital Preservation Maturity of the OPM. The specific objectives are: to assess the commitment of the OPM, sustainability and adequacy of its resources in ensuring effective digital preservation; to establish the extent to which the repository and preservation environment of the OPM adheres to the accepted operational practices of ISO 14721 and ISO 16363 respectively; to establish the extent to which the integrity, security, usability and accessibility of digital records is assured when undertaking business actions, and finally, to determine the roles of producers and users from creation, transfer as well as the use of the digital records at the OPM. This study will employ a qualitative case study, whereby at the EDRMS division, all the (9) employees will be selected. In each of the OPM departments, one (1) employee that frequently use the system will be purposefully selected. All the 12 Departmental Head will participate in the study. The total sample being 33.

Based on the above, I am hereby requesting your office to give the student the necessary support to collect data for the above mentioned study. The approved proposal for the study, is attached to this letter for your perusal.

For any further enquiries, please do not hesitate to contact me on the contact details provided.

Yours sincerely,



Prof. T. Kalusopa
Supervisor
Department of Information and Communication Studies
Office: 061 206 4776
Cell: 081 614 1870

Appendix D: Office of the Prime Minister Research approval letter

REPUBLIC OF NAMIBIA

OFFICE OF THE PRIME MINISTER

Tel No: (061) 287 9111
Fax No: (061) 234 296

Private Bag 13338
WINDHOEK

Enquiries: Mr. David Lyeengolo
Tel: 061-2872149

22 July 2020

Mr. Asser Laudika Napandulwe Nakale
P. O. Box 24332
Windhoek
Namibia

Dear Mr. Nakale

RE REQUEST FOR APPROVAL TO CONDUCT ACADEMIC RESEARCH WITHIN THE OFFICE OF THE PRIME MINISTER.

Your application to conduct academic research within the Office of the Prime Minister has been approved. Upon completion of your research you are expected to share the report with the Office.

The research must be anonymous to any individual, and must be shared with the Office of the Prime Minister prior to publication.

Yours Sincerely

OFFICE OF THE PRIME MINISTER
EXECUTIVE DIRECTOR

I-BEN NATANGWE NASHANDI
EXECUTIVE DIRECTOR

All official correspondence must be addressed to the Executive Director

Appendix E: Informed Consent Form

PARTICIPANT INFORMATION LEAFLET AND CONSENT FORM

ANNEX 5

TITLE OF THE RESEARCH PROJECT:

Assessment of the Digital Preservation Maturity at the Office of the Prime Minister of Namibia

REFERENCE NUMBER: 201201492

PRINCIPAL INVESTIGATOR: Asser Laudika Napandulwe Nakale

ADDRESS: P O Box 97738, Maerua Mall, Windhoek

CONTACT NUMBER: 0812878177

You are being invited to take part in a research project. Please take some time to read the information presented here, which will explain the details of this project. It is very important that you are fully satisfied that you clearly understand what this research entails and how you could be involved. Also, your participation is **entirely voluntary** and you are free to decline to participate. If you say no, this will not affect you negatively in any way whatsoever. You are also free to withdraw from the study at any point, even if you do agree to take part.

This study has been approved by the Research Ethics Committee at The University of Namibia and will be conducted according to the ethical guidelines and principles of the international Declaration of Helsinki, South African Guidelines for Good Clinical Practice and Namibian National Research Ethics Guidelines.

1. What is this research study all about?

This study will be conducted at the Office of the Prime Minister (OPM) in Windhoek. The main interest is the EDRMS Division, but all 12 Divisions of the OPM constitute the population of the study. 12 Heads of Departments (one from each of the identified departments) will be sampled, who will then refer the researcher to 1 user (preferably the most frequent user of the system) per department. All 9 employees of the EDRM Division also form part of the sample, bringing the total sample to 33 participants.

This study aims at investigating and assessing the extent to which digital preservation is carried out at the OPM and determine its level of Digital Preservation Maturity. This study would generate results that OPM could use to develop strategies as well as a road map for incremental capability improvement and measure their status against fellow organizations. In addition, it would create awareness not only for OPM, but other organizations involved in digital preservation on issues related to effective digital preservation. Equally important, the study could contribute to the body of knowledge on digital preservation, particularly the area of Digital Preservation Maturity.

Should you accept to partake, I will make an appointment with you. During interviews, open-ended questions will be posed to you, leaving room for better explanations. With your permission, a recording device may be used throughout the interview to capture the information.

2. Why have you been invited to participate?

With the main objective of the study being to assess the Digital Preservation Maturity of the OPM, an input from all the departments of the OPM at different levels is of outmost relevance for this study. The findings of this study will only be relevant if they include information from different departments of the OPM and at different levels. Therefore, I find it relevant to invite you to partake in the study.

3. What will be expected of you?

As a participant in this study, I would like to invite you to respond to questions during the interview. If anything is unclear, please do not hesitate to ask for clarification during the interview. This interview is expected to take not more than an hour.

4. Will you benefit from taking part in this research?

Partaking in this study does not come with any personal benefits. However, the study will produce outcomes which will help the OPM, stakeholders and other Organisations involved in Digital Preservation on issues related to effective digital preservation. Equally important, the study could contribute to the body of knowledge on digital preservation, particularly the area of Digital Preservation Maturity.

5. Are there in risks involved in your taking part in this research?

Please note that there are no risks involved in taking part in the study.

6. If you do not agree to take part, what alternatives do you have?

Your participation in this study is voluntary and you can withdraw from this research at any time with no negative consequences.

7. Will you be paid to take part in this study and are there any costs involved?

Your participation is free and no reward offered will be. Any costs involved are a responsibility of the Researcher.

You can contact the Centre for Research and Publications at **+264 061 2063061; pclaassen@unam.na** *if you have any concerns or complaints that have not been adequately addressed by the investigator.*

You will receive a copy of this information and consent form for your own records.

11. Declaration by participant

By signing below, I …….. agree to take part in a research study entitled *(insert title of study)*.

I declare that:

a) I have read or had read to me this information and consent form and it is written in a language with which I am fluent and comfortable.
b) I have had a chance to ask questions and all my questions have been adequately answered.
c) I understand that taking part in this study is **voluntary** and I have not been pressurised to take part.
d) I may choose to leave the study at any time and will not be penalised or prejudiced in any way.
e) I agree/decline to be recorded during the interview.
f) I agree/decline to be observed during the observation period.

Signed at (*place*) ..... on (*date*) …….. 2021.

…… ……

Signature of participant Signature of witness

12. Declaration by investigator

I Asser Laudika Napandulwe Nakale declare that:

- I explained the information in this document to ……..
- I encouraged him/her to ask questions and took adequate time to answer them.
- I am satisfied that he/she adequately understands all aspects of the research, as discussed above
- I did not use an interpreter

Signed at Windhoek on (*date*) ……..…….. 2021

…… ……

Signature of investigator Signature of witness

Appendix F: Interview guide for the Heads of Records

Section 1: Digital preservation infrastructure

1.1 Digital Preservation Policy

- Do you have a digital preservation policy in place?
- If no, are there any plans to come up with a digital preservation policy?
- Does not having a digital policy affect you in any way?
- If yes, what does the policy entail?
- How often does the policy get audited for compliance?
- Is the policy communicated to all stakeholders?

1.2 Digital Preservation Strategy

- Do you have a formal strategy that addresses technology obsolescence?
- If yes, what exactly does it address?
- Does the strategy call for producers to convert electronic records to "preservation ready" formats OR does it allow records in native format?
- Are changes in technologies being monitored?

1.3 Governance

- Is there any formal information governance which assigns accountability and authority for digital preservation?
- Is there any Governance framework to ensure compliance of preservation repository, with applicable laws regulations, records retention schedule, disposition authorities and standards?

1.4 Collaboration

- Does the organisation have in place, a framework that allows it to collaborate with standing partners? e.g. IT, peer organization, software and service providers and support functions.
- If not, are there any plans to collaborate with any other entities in the future*?* With who?
- If yes, how many stakeholder entities have you so far collaborated with to address the digital preservation requirements?
- How often do you monitor or update the digital preservation framework to support reaching out to all stakeholders to identify and meet their digital preservation requirements?

1.5 Technical expertise

- Do you have qualified personnel for the positions involving Records Management?
- Do your employees have any operational access to specialized professional technical expertise?
- What measures do you have in place to make sure that your staff is up to date with necessary expertise?

1.6 Designated community

- Is there any formal document that defines rights, obligations and responsibilities of your designated community for electronic records to be transferred to the repository?

- Are there written agreements between users, producers and the repository in terms of rights, obligations and responsibilities as far as transfer, custody and dissemination is concerned?

1.7 Electronic Records Survey

- Has the organization ever carried out an electronic records survey?
- How often is it done?

Section 2: Digital preservation repository

2.1 Integrity

- Does the repository have a documented procedure for integrity protection of electronic records?

2.2 Security

- Does the organisation have a written disaster preparedness and recovery plan?
- What are measures in place to ensure that no records are lost, in case of any emergencies?
- Are there other measures in place to ensure security of electronic records from loss, theft or unauthorized access?

2.3 Preservation metadata

- How do you ensure that metadata of electronic records remain intact throughout all the preservation actions?

Section 3: Digital preservation services

3.1 Ingest

- Does the repository have any agreement with producers in place with regards to format, integrity, virus checks, metadata checks and quality?

Appendix G: Interview guide for the Records Management staff

Section 1: Digital preservation infrastructure

1.2 Digital preservation policy

- Are you guided by any policy as far as digital preservation is concerned?

1.3 Digital preservation strategy

- Are you aware of any formal strategy that addresses technology obsolescence?

1.4 Governance

- Are you aware of any Governance framework to ensure compliance of preservation repository, with applicable laws regulations, records retention schedule, disposition authorities and standards?

1. 5 Collaboration

- Do you collaborate with any other organization/entity in terms of electronic records management?

1.6 Technical expertise

- Have you ever received any training with regards to electronic records management?
- Do you have any operational access to specialized professional technical expertise?
- If yes, internal or external?
- What exactly does it help you with?

Section 2: Digital preservation repository

2.1 Open Standards Technology Neutral Formats

- Have you adopted any file format as a preferred preservation format?
- If no, why not?
- If yes, what is your preferred preservation format?
- How many of the preferred formats are OS/TN formats?

2.2 Integrity

- Does the repository have a documented procedure for integrity protection of electronic records?
- How does the repository ensure integrity of electronic records throughout all preservation actions?

2.3 Security

- Do you have a written disaster preparedness and recovery plan in place?
- If yes, does it support all functions of ISO 14721 preservation repository?
- What security measures do you have in place to ensure security of electronic records from loss, theft and/ or unauthorized access?

2.4 Preservation metadata

- How do you ensure that you capture and maintain metadata of electronic records throughout the preservation actions?

Section 3: Digital preservation services

3.1 Ingest

- During ingest, is the content description (metadata) checked manually or the system does it automatically?

3.2 Access

- Does the repository allow/support access to electronic records?
- If no, why not?
- If yes, how and in what format?

Appendix H: Interview guide for IT personnel

Section 1: Digital preservation Infrastructure

1.1 Digital Preservation Strategy

- Are you aware of any strategy that addresses technology obsolescence?
- Are changes in technology being monitored?

Section 2: Digital preservation repository

2.1 Open Standards Technology Neutral Formats

- Has the repository adopted any file format as a preferred preservation format?
- If yes, what is your preferred preservation format?
- Do you have any technology watch program in place to monitor the sustainability of these formats?

2.2 Device/Media Renewal

- Does the repository have a formal media renewal protocol in place?
- If yes, how often is it mandated
- Apart from renewing readability, what else does it address?
- Does the system automatically monitor the potential loss of readability?

2.3 Integrity

- Does the system generate Hash Digests?
- If no, what technique do you use to ensure integrity of electronic records?

2.4 Security

- What measures do you have in place to ensure the safety and security of electronic records in case of any emergencies?
- Are there other measures in place to ensure the security of electronic records from loss, theft or unauthorized access?

2.5 Preservation metadata

- How do you ensure that metadata of electronic records remains intact throughout all the preservation actions?

2.6 Archival storage

- How many instances of the preservation repository support the storage of AIPs?

Section 3Digital preservation services

3.1 Ingest

- During ingest, is metadata checked manually or the system does it automatically?

3.2 Access

- Does the system have an integrated search functionality?" If yes,
- How does it work?

Appendix I: Interview guide for users

Section 1: Digital preservation infrastructure

1.1 Technical expertise

- Are you able to use the EDRMS?

1.1 Designated community

- Have you ever signed any agreement with the repository?
- Were you ever engaged by the repository regarding the establishment of any agreement?

1.1 Electronic records survey

- Have you ever participated in an electronic records survey? (To identify preservation ready, near preservation ready and legacy permanent electronic records in the custody of all records producers? If yes,
- How many times?

Section 2: Digital preservation repository

2.1 Open Standards Technology Neutral Formats

- Are you required to upload your records in a certain format?
- Which format?

2.2 Preservation metadata

- Does the system automatically capture metadata or do you enter it manually?

Section 3: Digital preservation services

.1 Ingest

- Do you sign any agreement with regard to format, integrity, virus checks, metadata checks and quality?

3.2 Access

- Does the system authorize access to the records? If yes,
- How?

Appendix J: Observation checklist

Observed	**Observed**	**Not observed**	**Comments**
Electronic records management/Digital preservation policies, manuals or guidelines			
Other governance frameworks			
Repository's engagements and agreements with stakeholders			
Collaboration framework			
Appropriateness of the security measures			
Users' ability to use the system. Documents uploading and retrieval.			
Users access the information stored on the system			
System's ability to detect loss of readability or Corruption			
Types of formats allowed/accepted by the system			
Sustainability of formats allowed/accepted by the system			

Appendix K: Document review checklist

Document	**Reviewed**	**Not reviewed**	**Comments**
Policies/drafts related to the EDRMS			
EDRMS user manual			
Collaboration agreements			
EDRMS-related Meetings agendas, minutes and reports			
Training manuals			
EDRMS related agreements			
Records survey questionnaires			