ASSESSING THE USE OF CLOUD COMPUTING FOR RECORDS MANAGEMENT IN SELECTED ORGANISATIONS IN NAMIBIA

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF ARTS IN RECORDS AND ARCHIVES MANAGEMENT

OF

THE UNIVERSITY OF NAMIBIA

BY

ALINA NDAPUNIKWA TALEINGE KARLOS

201045257

APRIL 2023

SUPERVISOR: PROF. C.T. NENGOMASHA (UNIVERSITY OF NAMIBIA)

ABSTRACT

This multi-case study assessed the use of cloud computing for records management in selected private organisations in Namibia. The study's objectives were to assess the drivers and benefits of adopting cloud computing for records management; analyse the cloud computing services and deployment models adopted by the organisations; assess the risks of managing records in the cloud; and identify measures to mitigate risks of managing records in the cloud. A qualitative research approach using semi-structured interviews was employed for data collection. The study population comprised of Namibian organisations using cloud computing and offering cloud computing services for records management. Four private organisations were conveniently selected. Seven participants comprising information technology (IT) staff from cloud computing service-providing organisations and records management staff from both a cloud computing service client organisation and a cloud computing service provider were purposively selected for the study. Data was analysed through content analysis. The study found that Namibian organisations adopted cloud computing for records management. However, cloud providers refered to information managed on the cloud as 'data'. The study findings established that organisations adopted cloud computing due to its flexibility and affordability. Significant lack of records management expertise in both cloud computing service providers and client organisations was evident. The study further established that records management legal and regulatory framework had not received comprehensive attention by both cloud computing service providers and client organisations. Namibia's current legal and regulatory framework is weak on the management of electronic records. The introduction of new laws relating to managing electronic records will be instrumental to the success of using cloud computing to manage records. The findings also highlighted that managing records in the cloud presented some risks and challenges such as non-compliance with laws, uncertain records security, and poor knowledge of records management. The study concluded that the cloud computing services provided and adopted by the Namibian organisations were not fully viable for the proper management of electronic records and there was a need for the customisation of cloud computing services to meet records management standards and practices. The study proposed a framework for adopting cloud computing for records management in Namibia.

Keywords: cloud computing, electronic records management, information and communication technology

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ADRI	Australian Digital Recordkeeping Initiative
APIs	Application Programming Interfaces
EDRMS	Electronic Documents and Records Management System
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
InterPARES	International Research on Permanent Authentic Records in Electronic Systems
IRMT	International Records Management Trust
ISO	International Organisation for Standards
IT	Information Technology
MICT	Ministry of Information and Communication Technology
MoReg	Model Requirements for the Management of Electronic Records
NamIGF	Namibia Internet Governance Forum
NAN	National Archives of Namibia
NSIT	National Institute of Standards and Technology
OAIS	Open Archival Information System
PaaS	Platform as a Service
RIM	Records and Information Management
SaaS	Software as a Service
SLA	Service Level Agreement
UNAM	University of Namibia

ACKNOWLEDGEMENTS

Firstly, I would like to thank God for his guidance and strength he granted me to complete this study. The completion of this study would not have been possible without the support and guidance of the following people and organisations:

- My supervisor Prof. Cathrine Nengomasha, for your advice, guidance and mentorship.
- My husband and daughter for supporting and granting me the time I needed to complete this study.
- The University of Namibia for tuition.
- The organisations that granted me permission to conduct the research and the individual participants.
- Mrs. Sarah Mwanandimai for editing.
- To all my friends and family that continuously believe in me.

However, I alone remain responsible for any weaknesses and shortcomings in this study.

DEDICATION

To my late grandmother, Meekulu Lusia Vatilifa for laying the education foundation to which I continue building on; and to my husband, Elisa Pombili Ndadi, for believing in me and motivating me to reach the highest heights of my academic career.

DECLARATION

I, Alina Ndapunikwa Taleinge Karlos, hereby declare that this is a true reflection of my own research and that this work or part thereof has not been submitted for a degree in any other institution of higher learning.

No part of this dissertation may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means without the prior permission of the author, or the University of Namibia.

I, Alina Ndapunikwa Taleinge Karlos grant the University of Namibia the right to reproduce this dissertation in whole or in part, in any manner or format, which the University of Namibia may deem fit, for any person or institution requiring it for study and research; providing that the University of Namibia shall waive this right if the whole dissertation has been or is being published in a manner not satisfactory to the University.

April 2023

Alina Ndapunikwa Taleinge Karlos Date

CHAPTER ONE

INTRODUCTION

1.1 Background to the study

Public and private sector organisations are gradually beginning to realise the benefits of storing and managing records in the cloud to accommodate the increasing electronic records created daily and address issues of access, security and confidentiality. However, the usage of cloud computing services in managing electronic records comes with major challenges to records management professionals many of whom are not well prepared for the management of such records.

Cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services" (Mell & Grance, 2011, p. 2). Gorelik (2013) outlines that cloud computing encompasses three service categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In addition, Rountree and Castrillo (2013) highlight that cloud services take on four forms of deployment models: private, public, community and hybrid cloud. Moreover, Rountree and Castrillo (2013) argue that each service and deployment model satisfies different organisational needs. Therefore, it is important for organisations to choose a service and model according to their needs and budget.

In the interest of this study, the International Records Management Trust (IRMT) (1999a, p.14) definition of records management is adopted as:

> *...that area of general administrative management concerned with achieving economy and efficiency in the creation, maintenance, use and disposal of the records of an organisation throughout their entire life cycle and in making the information they contain available in support of the business of that organisation.*

For records and information management (RIM) professionals, cloud computing resembles a traditional hosting service: information storage or applications are outsourced to a third-party provider and accessed by the organisation through a network connection (Ferguson-Boucher, 2011). However, the information, applications and processing power in the cloud are distributed across many servers and stored along with other clients' data, separated only by logical isolation mechanisms, which presents both new records management challenges and benefits.

E-governance activities and the rapidly increasing use of technology in conducting business led to the creation of large volumes of electronic records both for public and private institutions. The management of electronic records presents institutions with challenges of costly IT infrastructure and systems as well as the need for IT expertise. In addition, it requires storage with long-term digital preservation, which most organisations are not equipped to deal with (Stuart & Bromage, 2010). Cloud computing offers solutions to these problems in the form of cutting cost, increased storage, on-demand self-service, broad network access, rapid elasticity, flexibility, scalability, security, compliance and digital preservation (Diaby & Rad, 2017).

Using cloud computing services for records management presents a variety of business and legal risks (Government of South Australia, 2015; Stuart & Bromage, 2010). Failure to comply with legislative requirements of another jurisdiction, unauthorised access, loss of access to records and unauthorised destruction, are some of those risks. Studies done in Namibia (Nghihalwa & Shava, 2018; Tjikongo & Uys, 2013) highlight general technical challenges such as IT infrastructure maintenance, high support outsourcing costs and tiresome infrastructural procurement processes. Ravanbakhsh (2010) claims that cloud applications may lack the capability to implement records disposition schedules, including the ability to transfer and permanently delete records.

Therefore, specific service and deployment models may not meet all the electronic records management requirements, for example, maintaining records functionality and integrity throughout their lifecycle, maintaining links between the records and their metadata, transfer of archival records to an archives or deletion of temporary records according to approved retention schedules. This threatens the long-term trustworthiness and sustainability of records. Fortunately, these challenges can be mitigated by including the records management staff in the planning, development, deployment, and use of cloud computing solutions.

Factors to consider in managing recordkeeping risks when using cloud computing services include assessing the capacity of the cloud service and model to perform recordkeeping functions, assessing risks for different record types, performing due diligence when selecting a cloud computing provider, service and deployment model, and establishing contractual arrangements to manage risks (Government of South Australia, 2015; Stuart & Bromage, 2010).

1.2 Context of the study

1.2.1 Namibia's Information and Communication Technology environment

The use of information and communication technology (ICT) to conduct business is dominating the 21st century and, globally, countries are inventing initiatives aimed at strengthening their information sectors for economic and social development (IST-Africa, 2018). Since Namibia gained independence in 1990, it has made great strides in developing its ICT sector. A dedicated Ministry of Information and Communication Technology (MICT) was established in 2008, with a mandate to "lay the foundation for the accelerated use and development of ICT in Namibia, and coordinate information management within Government" (IST-Africa, 2018; Ministry of Information and Communication Technology, 2017, p. 6). According to Vision 2030, the Namibian government aims to transform Namibia into a knowledge-based society and leverage knowledge and technology for the benefit of the people (Office of the President, 2004). The Namibian government has initiated the roll-out of e-governance platforms across strategic state sectors and departments, and the review of ICT-related laws and policies with the aim of establishing appropriate legal frameworks for achieving the country's digital goals of vision 2030 (Namibia Internet Governance Forum (NamIGF), 2017). IST-Africa ranks Namibia's ICT infrastructure among the best in Africa (IST-Africa, 2014). To understand the use of cloud computing for records management in Namibia, it is vital to understand Namibia's current ICT context. According to the African Union (2022), Namibia has an exceptionally well-developed communications infrastructure.

- In 2019, the number of telephone lines was 5.6 /100 inhabitants, with 63 314 fixed broadband subscriptions compared to only 134 in 2005, registering an average annual rate of 162.65%.
- Only about half the Namibian population has access to the internet, to date, internet penetration stands at just over 51% of Namibians having access to the internet (NamIGF, 2021).
- Mobile cellular subscriptions of Namibia increased from 82 000 in 2000 to 2.82 million in 2019, growing at an average annual rate of 22.05%.
- There were 1.28 million internet users in Namibia in January 2020.
- Internet penetration stood at 51% in January 2020.

1.2.2 Namibia's legal and regulatory framework for electronic records management

Legislation plays a significant role in records management in all media formats. Many countries have laws governing the management of records with a direct stand on the management of electronic records. Such laws may include records and archives acts and policies, e-commerce laws, freedom of information and privacy, or data protection laws. The Archives Act (Act 12 of 1992) to preserve state records and make them accessible to the nation mandates the National Archives of Namibia (NAN). NAN is the institution responsible for providing leadership and guidance on information governance practice in all institutions governed by an Act of Parliament. Namibia does not have all the laws for managing records, such as the freedom of information act and data protection or privacy laws. The following is a summary of the two key laws that affect the management of records in Namibia:

a) Archives Act 12 of 1992 "provides for the custody and care of and control over archives in Namibia and for matters incidental thereto". The Act defines a document as: a combination of any media and the information contained thereon or therein, including on paper, parchment, vellum, files, scrolls, or in the form of punched tape, magnetic tape, compact disc, photographic negatives and copies, cinematographic film, microfilm, microfiche, or gramophone, phonographic or other kind of sound recordings. This definition relates to both paper and electronic records. NAN further has an archives code issued by the head of archives in terms of article 12 of the Archives Act. NAN is reviewing the Act and the code and will develop a records and archives management policy for Namibia to directly address issues relating to electronic records management.

Although the Archives Act does not apply to private organisations, organisations providing cloud computing services to the public institutions would be bound by it.

a) The Electronic Transaction Act 4 of 2019 was enacted to:

"provide for a general framework for the promotion of the use of electronic transactions in the Republic of Namibia; provide for the legal recognition of electronic

transactions; provide for the admission of electronic evidence; provide for consumer protection in electronic commerce; regulate the liability of service providers for actions of their clients; and provide for matters incidental thereto" (Office of the Prime Minister, 2019, p1).

The Electronic Transaction Act defines "data evidence" as evidence of any matter relevant in legal proceedings, which is represented in a computer system directly and can be made readily understandable to a human being without requiring any special skills or knowledge on the part of any person and includes a display, print out or other output of that data. The Act further established an Electronic Information Systems Management Advisory Council to exercise the powers and perform the functions conferred on and assigned to it by or under this Act. The Act requires organisations to meet certain records keeping requirements for "data evidence" to be acceptable in a court of law.

1.2.3 Cloud computing in Namibia

The presence of cloud computing has made rounds in the local media and on IT solutions organisations' websites. Organisations offering cloud computing in Namibia include Green IT Solutions, the Document Warehouse, Technology Warehouse, Click Cloud Services, Connect Technologies, Dimension Data, Business Connexion, Salt Essentials and MTC Namibia. According to their websites, these organisations provide various cloud services that include SaaS, IaaS and PaaS and various deployment models (private, public, community and hybrid). These organisations praise the move to cloud computing for its enormous flexibility and affordability. The organisations include the four, which took part in this study, but cannot be named because they requested to be anonymous. Despite the various organisations using cloud computing in Namibia, only one client organisation agreed to participate in the study. The adoption of cloud computing in Namibia will enhance the chances of achieving one of Namibia's Vision 2030 objective of 'connecting all citizens by providing services through new technological horizons'. Chitauro (2017) identifies various organisations providing cloud computing services to the Namibian public and private organisations. However, Nghihalwa and Shava (2018) found that Namibian government IT departments feared the adoption of cloud computing due to security and privacy issues, complexity of technology and the mere fact of trusting an outsider to manage government records. These fears are not foreign to private organisations.

The four private organisations that participated in this study are in Windhoek, the capital of Namibia. These organisations have requested for anonymity in the participation agreements. Organisation A provides paper records storage and records management software, including cloud computing services. Organisations B and C provide various technology solutions, including data storage and cloud computing. Organisations A, B and C provide these services to both public and private organisations. While organisation C provides human resource services and uses cloud computing services to store and manage its information.

1.3 Statement of the problem

Requirements for records storage and addressing electronic records-keeping requirements are the drivers of organisations' adoption of cloud computing. Managing electronic records efficiently is essential to realising Namibia's Vision 2030. Several studies (Bassett, 2015; Duis, 2014; Stuart & Bromage, 2010) report benefits and risks of using cloud computing for records management. The benefits include reduced costs, increased productivity and improved business processes. The risks also include loss of records, privacy and security issues, non-compliance to legislation and unauthorised destruction of records. Avoiding many of the risks depends largely on the service and deployment model adopted.

This study investigated these issues of records management in cloud computing in four-selected organisation in Namibia. Studies (Nghihalwa & Shava, 2018; Tjikongo & Uys, 2013; Chitauro, 2017) conducted in Namibia discussed cloud computing's technicalities and did not bring in the aspects of managing records in the cloud.

This study investigated how issues of records management were considered in cloud computing by conducting a detailed study to assess the use of cloud computing for records management in Namibia. Such issues of records management in the cloud as identified by similar studies done in Africa are: accessibility of records in the cloud, security and confidentiality, compliance and long-term digital preservation (Kibe, 2016; Mosweu, Luthuli & Mosweu, 2019; Asogwa, 2012; Mosweu, 2012, Ngoepe & Saurombe, 2016). Failure to address records management requirements in cloud computing adoption could lead to a loss of e-records or loss of their usability. Organisations might fail to comply with Namibian laws pertinent to records management such as the Archives Act 12 of 1992 and the Electronic Transaction Act 4 of 2019.

1.4 Objectives of the study

This study's aim was to assess the use of cloud computing for records management in Namibia using cloud computing services and deployment models. The objectives of the study were to:

1.4.1. Analyse the cloud computing services and deployment models adopted by the selected Namibian organisations;

1.4.2. Assess if the factors which have driven the selected Namibian organisations to adopt cloud computing are related to records management;

1.4.3. Assess the risks of managing records in the cloud experienced by the selected Namibian organisation; and

1.4.4. Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations.

1.5 Significance of the study

The findings of this study, which assessed cloud computing for records management in selected organisations in Namibia, may contribute to policy formulations and practice on how successfully cloud computing can be used for records management. Additionally, the findings may aid the participating organisations in improving their approach to cloud computing for records management. Furthermore, the findings of the study contribute to the existing body of knowledge on cloud computing and records management, especially in the Namibian context.

1.6 Limitations of the study

This multi-case study design of four private organisations findings cannot be generalised to the entire Namibia. Although, they can be useful to the whole country. The Covid-19 pandemic presented a further limitation to the study, as interviews were conducted virtually, preventing observations to verify the data from interviews, which would have enhanced the findings' trustworthiness.

1.7 Delimitations of the study

This study focused on four private organisations, as cloud computing is widely provided by private organisations in Namibia.

1.8 Research Methodology

The study adopted a multi-case research design within an interpretivist research paradigm, applying a qualitative research approach. The qualitative approach was appropriate for this study as it focuses on understanding humans from multiple perspectives and it is flexible, which helps in addressing concerns in situations where little is known about the topic (Bricki & Green, 2007; Burton, 2000), as is the case with assessing the use of cloud computing for records management in Namibia. The population of the study was Namibian organisations providing or using cloud computing for records management. The sample was four Namibian private organisations providing and using cloud computing that were willing to participate in the study. Non-probability sampling using purposive method was employed to select participants, IT and records management staff, because of their direct involvement with records management and cloud computing.

The data collection methods were interviews. Semi-structured interview guides were used to collect data from IT and records management staff. The researcher obtained research permission from the Centre for Postgraduate Studies at the University of Namibia (UNAM) to conduct the research, which was used to obtain authorisation to conduct the study in the four organisations. Data from interviews were analysed using content analysis and presented in descriptive narrative.

1.9 Definition of key terms

This section defines keywords used in the study.

Cloud computing: cloud computing is an IT approach that provides convenient computation, software, data access, and storage services with minimal end-user management effort or interaction (Oppenheim, 2012; Mell & Grance, 2011).

Records management: the area of administrative management concerned with achieving economy and efficiency in the creation, maintenance, use and disposal of an organisation's records throughout their entire life cycle and in making the information they contain available in support of the business of that organisation (IRMT, 1999a).

Electronic records: refers to electronic information created, received, and maintained as evidence by an organisation or person, in pursuance of legal obligations or in the transaction of business and depend on computer hardware and software for access including emails, word processing database, webpages, digital images video and audio files, etc. (IRMT, 1999a; Marutha & Ngulube, 2012).

1.10 Structure of the thesis

This section outlines how the thesis is structured.

Chapter 1: Introduction – provides the study background, context of the study, problem statement, objectives, methodology and definition of terms.

Chapter 2: Literature Review and Conceptual Framework – discusses the literature and concepts significant to the study.

Chapter 3: Research Methodology – discusses research design, data collection methods and instruments, population and sampling and procedures. It further discusses reliability and validity, data analysis, ethics and methodology evaluation.

Chapter 4: Data Analysis and Presentation – analyses and presents data collected.

Chapter 5: Discussion and Interpretation of Research Findings – discusses data presented in chapter four with relation to literature.

Chapter 6: Summary of Findings, Conclusions and Recommendations – provides the summary of findings, conclusions and recommendations derivED from the study.

1.11 Summary

The chapter gave the background to the study by highlighting the current Namibian ICT infrastructure. The problem statement outlines how the increased use of ICT in the conduct of business led to the creation and management of vast electronic records that require costly ICT infrastructure and systems, driving organisations to adopt cloud computing. This chapter further looked at the study’s objectives, significance, limitations and delimitations. The methodology of the study was also briefly provided in this chapter and key terms were defined. The next chapter presents the literature review and conceptual framework.

CHAPTER TWO

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

2.1 Introduction

Literature review enables a researcher to develop a clear understanding of the research topic, establish what has already been researched on the topic and identify gaps, which the researcher's own study can fill. It highlights concepts and theories on the subject area (Bless, Sithole & Higson-Smith, 20013). The study evaluated literature from related studies and policies and guidelines of institutions employing cloud computing services. The conceptual framework based on cloud computing services and deployment models, guides the literature review. The organisation of this literature review is according to the study's objectives and the conceptual framework.

2.2 Characteristics of cloud computing

Cloud computing consists of five very important characteristics, which identify the unique properties that make cloud computing what it is and makes it distinct from other similar services. Diaby and Rad (2017) present these characteristics shown in Figure 2.1.

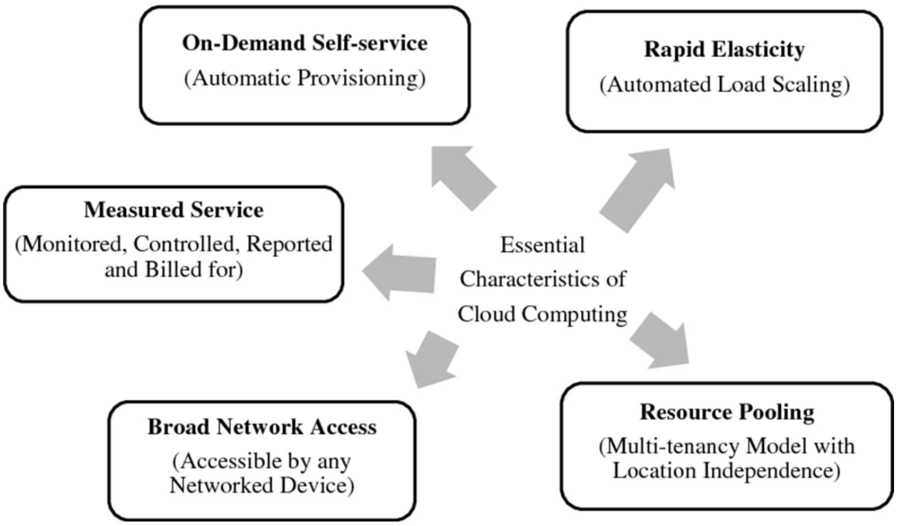

On-Demand Self-service
(Automatic Provisioning)
Rapid Elasticity
(Automated Load Scaling)
Measured Service
(Monitored, Controlled, Reported and Billed for)
Essential Characteristics of Cloud Computing
Broad Network Access
(Accessible by any Networked Device)
Resource Pooling
(Multi-tenancy Model with Location Independence)

Figure 2.1: Essential characteristics of cloud computing

Source: Diaby and Rad (2017)

Cloud computing's characteristics have an impact on records management in the cloud. Researchers (Mell & Grance, 2011; Diaby & Rad, 2017) also found these characteristics of importance in the discussion of cloud computing and records management.

2.2.1 On-demand self-service

On-demand self-service refers to the independent provision of computing capabilities such as storage by a client automatically when required without the need of human interaction with every service provider. Alrowaihi (2014) explains that the provision of cloud resources must be on-demand whenever the users require them and need to be accessed through an online control panel. Such resources include processing power, server time, storage, network access, web applications and virtual machines. The flexibility of acquiring cloud computing resources automatically has a significant impact on records storage, as organisations can increase and decrease the resources according to the quantity of records they are producing.

2.2.2 Resource pooling

The cloud provider pools resources to serve multiple clients at the same time using a multi-tenant model, with different physical and virtual resources dynamically allocated and reallocated according to client specifications. The client has no knowledge or control over the location of the resources, but can specify location at a higher concept such as country or data centre. Such resources can include memory, storage, and processing or network bandwidth (Mell & Grance, 2011; Puthal et al., 2015). This feature gives organisations the right to specify and know the location of the data centre where their records are stored.

2.2.3 Rapid elasticity

Computing capabilities can be rapidly released and distributed, as well as automatically distributed to meet the demand and scalability requirements. To the client, these computing capabilities can be altered at any time and appear unlimited allowing any quantity to be adopted. Puthal et al. (2015, p. 117) state, “a client can rapidly gain more resources from cloud by scaling out and can scale back in by discharging those resources once they are no more needed”. According to Mosweu et al. (2019), storage in the cloud is limitless and an organisation gets resources for storing records without additional hardware and installation into a local data centre.

2.2.4 Broad network access

Computing capabilities are readily available over the network and accessed through standard mechanisms that use varied thin or thick client platforms, for example mobile phones, tablets, laptops and workstations. Clients can access cloud resources over the internet anytime from anywhere through a variety of devices (Rashid & Chaturvedi, 2019). Kibe (2016) found that cloud-based services save on transmission time of the records, hence, accelerate the decision-making process in the public institutions in Kenya. In addition, cloud-based services facilitate the realisation of multi-user access to records, thereby enabling ready access to records and real-time collaboration in decision-making and task performance, as the records can be accessed outside the physical office environment.

2.2.5 Measured service

Cloud services automatically optimise and control resources through a pay-per-use system at the level of abstraction where the service is. Both the client and the provider monitor resources usage, which provides transparency for both parties. This implies that just like electricity or municipality water, IT services are charged per usage metrics – pay per use. The more you utilise IT, the higher the bill (Prasath, Gnanaraj & Ganesh, 2013). This helps organisations to save costs on IT infrastructure and expertise needed for the storage and management of electronic records.

Cloud computing characteristics help organisations to know what cloud computing is and what it does before adoption. Mell and Grance (2011) argue that when an organisation is adopting cloud computing service(s), it should consider the availability of these characteristics. Section 2.4 discusses in detail how these features of cloud computing benefit records management.

This study sought to find out the characteristics in the cloud computing deployment models and services used and provided to/by Namibian organisations that distinguish from other services and the impact they (characteristics) have on records management to address the study objective: 'To analyse the cloud computing services and deployment models adopted by the selected organisations in Namibia'.

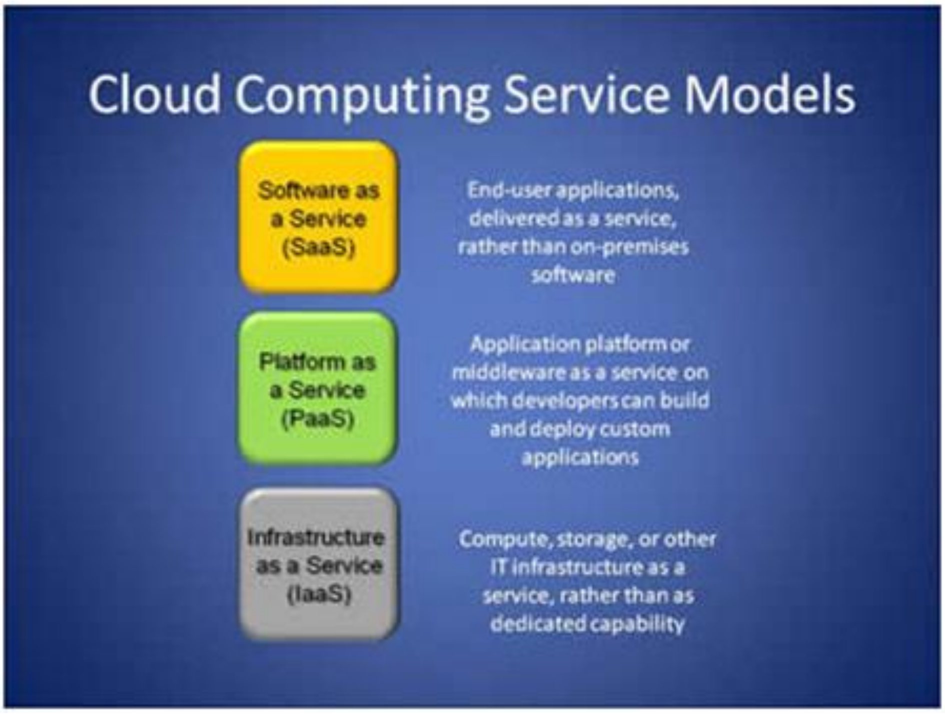
2.3 Conceptual Framework

2.3.1 Cloud computing services and deployment models

The conceptual framework for this study is the cloud computing services and the deployment models. Various scholars have argued that the success of cloud computing for records management is highly depends on the service and deployment model adopted by an organisation (Gorelik, 2013; Rountree & Castrillo, 2013; Diaby & Rad, 2017).

2.3.1.1 Cloud computing services

Cloud service models describe how cloud providers deliver cloud services to clients. Gorelik (2013) discusses three service models IaaS, PaaS and SaaS. The service models are made based on modern-day data centres that integrate the three models and provide them as utilities by letting clients pay only for what they use (pay-per-use). The figure below displays what each service offers to clients.


Cloud Computing Service Models

Software as a Service (SaaS) — End-user applications, delivered as a service, rather than on-premises software

Platform as a Service (PaaS) — Application platform or middleware as a service on which developers can build and deploy custom applications

Infrastructure as a Service (IaaS) — Compute, storage, or other IT infrastructure as a service, rather than as dedicated capability

Figure 2.2: The three most common cloud computing services

Source: Somepalle (2015)

2.3.1.1.1 Infrastructure-as-a-service (IaaS)

IaaS refers to the online delivery of virtual infrastructure elements such as servers, storage and network access (Government of South Australia, 2015). Low (2012) describes it as the provision of hardware, thus clients lease rather than obtain the IT infrastructure on an as-needed basis, allowing it to increase infrastructure capability easily and rapidly when necessary. IaaS providers offer hardware and the basic minimum software for users to develop on, such as virtual servers, storage systems, networking equipment and data centre space. Users have broad control over the services offered by IaaS providers as they can implement and run multiple software that might be needed such as operating applications and systems (Gaur et al., 2017).

This service allows the client to move the information workload, in its entirety to the providers' data centre. By using this service, clients share resources such as hardware (storage) and network (virtualisation and scalability), which allow for multi-tenancy with various applications, making it possible to share the same physical resources without competing (Mohamed & Pillutla, 2014). In this service, the client does not manage the underlying cloud infrastructure, but may have control over operating systems and applications.

2.3.1.1.2 Platform-as-a-service (PaaS)

In PaaS, the client develops and deploys applications in a cloud environment using specific tools and languages provided by the service provider. Government of South Australia (2015) describes this service as the online delivery of custom application development or deployment environments in which applications can be built and run on the service provider's systems. PaaS providers give users very little control over their software and programming environment. This is because PaaS providers implement a software layer over the hardware they offer, forcing users to work with the providers' software layer. This is beneficial to clients because the provider reduces the technical expertise needed for users to create their own web applications.

Developers can build custom web applications without installing any tools on an organisation's computers and then deploy those applications without requiring specialised system administration skills. The cloud service provider supplies the infrastructure required. The client has control over the deployed applications and possibly the configuration settings for the environment (Somepalle, 2015). Mohmed and Pillutla (2014) argue that applications such as content management, records management, collaborative platform and social media can be developed in this service type. In agreement, Youssef (2012) opines that PaaS allows clients the opportunity to design, model, develop and test applications directly on the cloud, therefore, giving a client control over the software lifecycle.

2.3.1.1.3 Software-as-a-service (SaaS)

In SaaS, the cloud provider supplies the facilities, infrastructure, hosted applications, and environment for personnel to use the cloud software via a web browser (Hidalgo, 2013). The client has no control over such software applications. SaaS providers ultimately offer software for multiple users over the Internet through a web browser. A good example of SaaS is Google Docs, where a user can edit documents through the software delivered over the internet. In simple terms, SaaS is a software offered by a third-party provider via the internet and is configured remotely. Today, SaaS is offered by companies such as Google, Salesforce, and Microsoft. The SaaS provider has complete control of the application software.

Applications are accessed from various devices through a client interface such as a web browser or through a program interface (such as web-based email) (Government of South Australia, 2015). Barnes (2010) argues that the adoption of cloud computing for records and information management continues to evolve with the aid of SaaS and electronic document and records management (EDRMS). The electronic document and records management system is defined as a type of content management system and refers to the combined technologies of document management and records management systems as an integrated system (New South Wales Government State Record, 2012). Convery (2010a), who describes SaaS as an area of "interest to the record and information management community for the future but adoption is dependent on evidence of the security of the cloud providers' services and infrastructure" (p. 8), supports this. Hidalgo (2013) argues that SaaS providers may have more knowledge in security than regular companies do since their focus is to protect their clients' data. On the contrary, Tolliver-Nigro (2009) cautions SaaS clients of SaaS vendor failings and security breaches that have occurred in the past. Organisations that choose SaaS providers should still do due diligence on the trustworthiness of the provider.

2.3.1.2 Cloud deployment models

Gorelik (2013) outlines four cloud deployment models: private, public, hybrid and community cloud. Choosing the suitable deployment model to be implemented by an institution is the first important step, as it promises a successful cloud computing implementation by that institution because different types of models require diverse skills and resources. Wrong choice of model will result in failure of the implementation process. Institutions must examine their data precisely, before deciding on the type of model to use to avoid implementation failure (Diaby & Rad, 2017). Below is the display of cloud computing models.

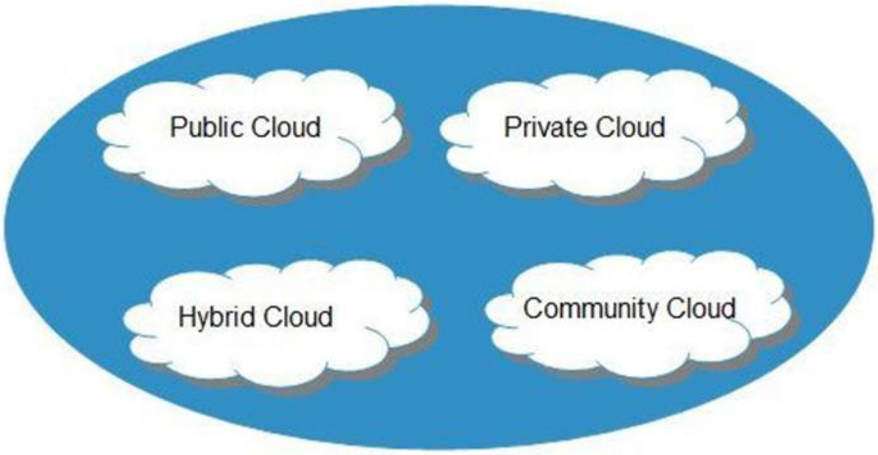


Figure 2.3: Cloud computing deployment models

Source: Somepalle (2015)

In a private cloud, computing resources are operated exclusively by one organisation and may be managed by the organisation itself. Mell and Grance (2011) argue that private clouds are considered more secure than public clouds since their users are trusted individuals in the organisation. This model might be the best model for records management as clients have more control and knowledge of the records storage location. It also addresses concerns of jurisdiction of records. Diaby and Rad (2017) reason that a private cloud is the most secure model as it offers enhanced security measures, dedicated resources and better customisation as data processes are controlled and managed in the organisation exclusive of any limitation of bandwidth network and security disclosures. A private cloud can be compared to intranet. However, with a private cloud the organisation incurs the costs of capital and operational resources, especially with on-premises private cloud.

A public cloud avails infrastructure and storage to the public over the internet. This does not mean the client's data will be openly exposed to be visible as the public cloud employs data separation to prevent one client from accessing another client's information (Gorelik, 2013). This cloud is owned by the providers and services are offered on a pay-per-use basis (Youssef, 2012). Nonetheless, public clouds are less secure compared to private clouds as all applications and data on the public cloud are prone to malicious attacks unless there are security checks implemented through validation from both providers and clients (Jadeja & Modi, 2012).

The other two deployment models, community clouds and hybrid clouds, fall between private and public clouds (Mell & Grance, 2011). Community clouds are similar to private clouds, but the cloud infrastructure and computing resources are shared by several organisations that have the same mission, policy and security requirements. An example of a community cloud is the educational cloud used by universities and institutions around the world to provide education and research services (Yousef, 2012). Rao, Leelarani, Kumar (2013) argue that a community cloud is a shared computing resource across organisations of similar business operations and requirements who seek to share infrastructure to realise some of the benefits of cloud computing while sharing cost. Google “Gov cloud” is a good example of a community cloud.

While a hybrid cloud is the cloud infrastructure consisting of a combination of two or more; public, private or community cloud components. The cloud components are bound together by standardised technology and managed as a single unit, yet each cloud remains a unique entity (Rountree & Castrillo, 2013).

2.3.2 Choosing a cloud service and deployment model for records management

Keeping up with endless technological evolution can be a challenging task. The loose definition of terms and industry-specific dialects make it even more difficult. King (2019) argues that the proper definition of enterprise technology solutions and associated terms have real implications to digital information management. Defining the terms related to electronic records management and cloud computing is thus necessary for this study. Data management is the process of storing, organising and maintaining the data created and collected by an organisation (Stedman & Vaughan, 2020). King (2019) argues that content management systems aim to achieve regulatory compliance and risk management, retention and dissemination of business knowledge, and cost and process efficiencies. On the other hand, records management is concerned with making sure organisations’ records are stored, organised, archived, and accessible over time while complying to regulatory frameworks (Rice, 2022). Regrettably, most organisations cannot afford to have separate solutions for the different information management functions.

Making the decision to move to the cloud is a complex task and it highly depends on organisational context. Different organisations will be satisfied by different services and deployment models depending on their organisational needs, operations and budget (Rountree & Castrillo, 2013; Diaby & Rad, 2017).

Cloud services and cloud deployment models guided this study to determine the success of using cloud computing services to manage records. Masud and Huang (2012) proposed a cloud implementation roadmap with four stages. In the first stage, an organisation must gather knowledge, do a feasibility study and plan, while in the second stage it must do an evaluation of the present stage and experiment on cloud usage. The third stage, which is critical to this study, involves choosing the right cloud computing service and deployment model and the last stage is the implementation and management of the solution. An organisation needs to establish its need for cloud computing services and determine if they offer the necessary features, experiment on cloud usage, choose the right cloud service provider and deployment model in order to migrate records to the cloud (Masud & Huang, 2012).

Diaby and Rad (2017) argue that successful cloud computing implementation depends on the choice of the right service and deployment model for each organisation. The study analysed the factors that organisations considered to determine the cloud service(s) and deployment model(s) to use for records management.

2.4 Potential benefits of cloud computing for records management

The rapid increase in the use of IT in institutions results in the generation of electronic records. Electronic records are informational files or data created, received, maintained, and stored in digitised form, using computers and applications software. Electronic records, according to Marutha and Ngulube (2012), are records that depend on computer hardware and software for access, including emails, word processing, database, webpages, digital images, and video and audio files. The management of electronic records presents institutions with challenges of spending on costly IT infrastructure and systems such as EDRMS as well as acquisition of IT expertise because of lack of massive storage space and technological evolution, leading to obsolescence (Stuart & Bromage, 2010). Kibe (2016) conducted a study on the impact of cloud-based services on records management in Kenyan public organisations, which found that most organisations had increasingly started using the cloud-based services to offer efficient and cost-effective technology solutions, while other organisations were moving to cloud-based records management to cut costs, eradicate redundancies and pool resources. Kibe (2016), however, advises organisations to weigh against the risks associated with privacy and security of records when choosing cloud computing services and deployment models for records management.

Cloud computing offers good records management solutions to records managers, as it facilitates fast delivery of information and provides huge space for the storage of records. Additional advantages associated with cloud computing for records management include cost saving, enhanced accessibility, better centralisation, increased flexibility, having access to records even in time of disaster, and improved interaction with the user community (Kibe, 2016; Mosweu et al. 2019). Another important benefit of cloud-based services is its capacity to facilitate remote access to records regardless of the physical location of the users.

Cloud computing offers organisations more choices regarding how to run infrastructure, save costs, and delegate liabilities to third-party providers. It has become an integral part of technology and business models, and has forced businesses to adapt to new technology strategies. However, organisations using or considering the adoption of cloud computing need to be aware of other factors that could negatively affect control of their records, such as records stored in unknown locations, problems when applying retention and disposal schedules, privacy and security risks (Duis, 2014). Risks could be minimised by involving records managers in deciding whether to go to the cloud, selecting a cloud provider and selecting the service and deployment model in collaboration with the IT department (Duis, 2014).

Cloud computing offers numerous potential benefits for records management, depending on the service and deployment model adopted. Bassett (2015) affirms that cloud computing benefits are organisationally contextual and depend on the type of cloud computing service and deployment model used. This means every organisation may not achieve every benefit of cloud computing, but has the potential to gain them under different circumstances. Cloud computing's potential benefits to records management are discussed below.

Carroll, Van der Merwe and Kotzé (2011, p. 4) identified 13 benefits of cloud computing as indicated in Figure 2.4.

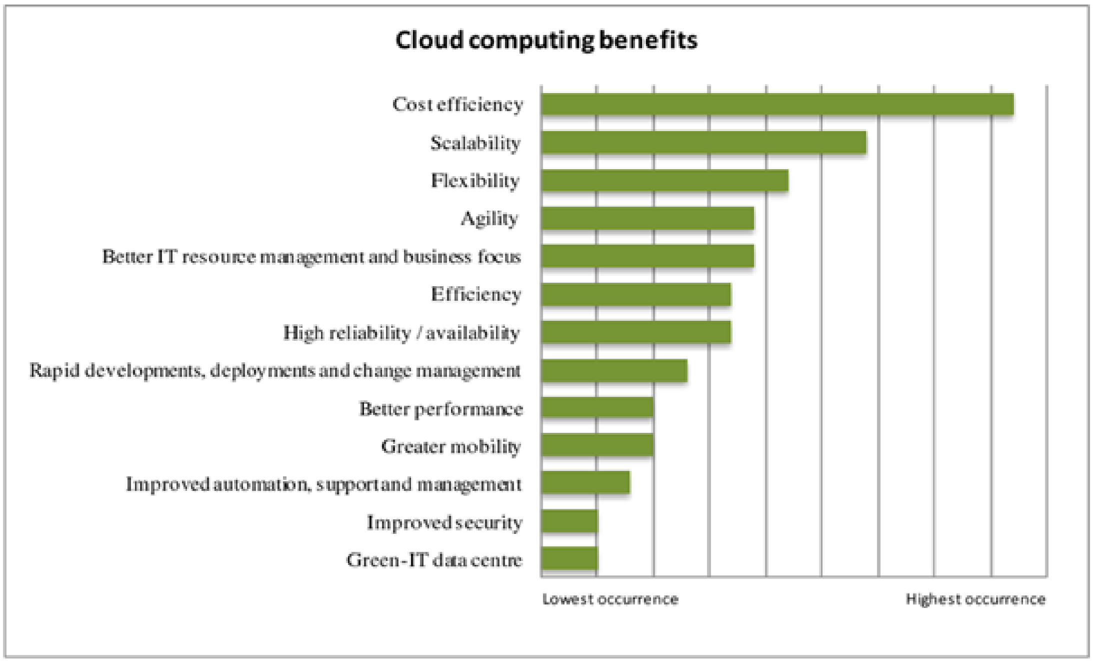


Figure 2.4: Cloud computing benefits

Source: Carroll et al. (2011, p. 4)

Literature (Carroll et al., 2011; Kibe, 2016; Bassett, 2015), suggest that the following nine are the most common potential benefits of cloud computing.

2.4.1 Cost efficiency

Cloud computing provides great savings in IT-related costs, both hardware and software. The organisation does not own the hardware used for storage, power, cooling and floor space. In most cases, organisations may not even know the actual physical location of the hardware (Carroll et al., 2011; Bassett, 2015). According to Bassett (2015), organisations using cloud computing do not have to pay licensing fees, or support and maintenance to use the software provided by cloud providers. Cloud computing also offers low operational cost as clients only pay for what is used (measured service) (Carroll et al., 2011). Furthermore, cloud computing further benefits the client with cost-cutting, as less IT staff are needed to help maintain internal systems and software because it is the providers' responsibility to maintain the technology. In addition, cloud-based services offer organisations massive storage space, as they enable organisations to save on the physical storage space (Kibe, 2016). Organisations can avoid high expenditure by paying only for computing resources they need on demand to keep systems running and perform business transactions instead of investing in their own data centres (which involves buying and maintaining software and hardware, providing secure facilities to house machines and employing personnel to keep it running), to meet increasing computing and storage capacity demands. However, cloud computing still involves costs to an organisation, as it integrates new services with existing legacy processes. This study aimed to establish how the adoption of cloud computing facilitated cost-cutting in Namibian organisations using cloud computing for records management.

2.4.2 Scalability and flexibility

Scalability means that cloud computing resources can be scaled up or down (increased or decreased) depending on the user's needs, while flexibility refers to the user's ability to obtain the resources they need, the time they need it (Convery, 2010a). This allows for better resource monitoring and rapid elasticity of resource provisioning (Mell & Grance, 2011). Convery (2010a) further argues that cloud services are highly elastic and allow clients to scale up computing power during high demand periods and down during low demand periods. A study conducted in Namibia by Chitauro (2017) found that organisations' reasons for switching to the cloud were to increase flexibility and scalability of IT resources.

The promise of unlimited resources on demand, however, needs to be tested cautiously to understand how quickly and the extent to which a cloud service provider can provide the up or down scaling capabilities. The usage of cloud resources is metered and organisations need to monitor them to ensure that running costs do not outweigh perceived benefits (Bassett, 2015). Although a cloud service provider may claim to provide unlimited resources on demand, their capability to scale these resources needs to be determined for the client (Convery, 2010a). The study investigated how scalable and flexible cloud resources adopted by the organisation and the clients were and how the service providers ensured the realisation of scalability and flexibility of cloud resources.

2.4.3 Modernisation of business processes

Cloud computing eliminates the need for organisations to go through lengthy procurement processes of acquiring licences for a provider's proprietary product when changing from traditional methods to modernised business processes. As an alternative, organisations can select new innovative and regularly updated applications and services, such as SaaS (Convery, 2010a). Cloud computing further provides the ability to integrate various cloud services to address businesses' short- and long-term needs. In addition, the availability of applications and services over the internet from everywhere facilitate collaborative working internally and externally through sharing of information and the ability to collaboratively edit documents in real time despite one's location (Convery, 2010a). Furthermore, Kibe (2016) agrees that cloud computing increases efficiency and effectiveness in service delivery, as technology is highly used in capturing, managing and processing of records compared to the case where systems are running manually.

Convery (2010a) states that there is decreased ability of customisation to cloud services and applications since they are mostly built to serve a wide customer base. It is, therefore, the client's responsibility to discuss customisation of services with the provider before deciding to determine whether there are services that can be tailored to the organisation's needs. The study analysed the improvement of business processes with the use of cloud computing, as improved business processes aid decision making in business.

2.4.4 Availability and reliability

Availability refers to the ability to provide always-accessible data and reliability refers to the reliability of the services. Convery (2010a) claims that the availability and reliability of cloud computing services are usually expressed to be at 99.9%, depending on the type of service. In the case where the cloud service provider's server fails, it would not automatically affect a client. Because of access to many computing resources, the service provider can switch automatically to another server. The clients' data is usually stored in multiple geographic locations to prevent information loss, server outages and for disaster recovery (Bassett, 2015).

The utilisation of cloud computing creates an always-on feature for access, which allows work to be done at any time and any location through the internet. A study by Kibe (2016) found that cloud-based services saved on transmission time of the records, therefore, speeding up the decision-making process in institutions. This is a critical benefit, as it speeds up service delivery due to the ability to provide the right records at the right time to the right person.

However, clients need to know that service providers can experience service outages, which clients cannot control and for which customers can only be compensated in free service time. These outages draw concerns to the viability of cloud computing for data storage and records management (Convery, 2010a). Despite its high availability and reliability, clients must note that there can still be outages that may be unacceptable for some organisations, thus the reputation of service providers must be considered. The study assessed how retrieval of records has improved with cloud computing.

2.4.5 Rapid development and deployment

As a cloud computing benefit, rapid development and deployment refers to the ability of cloud computing to provide pre-tested, configured and installed software. Software is promptly availed by the provider after the client signs up for the cloud service. Therefore, providers can deploy new applications and/or services much quicker than the client could do it on their own (Ferguson-Boucher, 2011). In cloud computing, resources are on-demand self-service features, where the client simply selects the services they require and provisions where they are needed. Another potential benefit is that in many cases there is no long-term commitment, as a client can try out a cloud service and cancel it if it does not address their needs (Convery, 2010a; Mell & Grance, 2011). This rapid deployment and resource management feature allows organisations to adapt to fluctuations based on their needs and can continue business operations with minimal limitations. The study evaluated how timely clients can select and discontinue resources in the cloud service(s) adopted.

2.4.6 Business continuity and disaster recovery

Business continuity and disaster recovery refers to an organisation's ability to maintain essential functions during and after a disaster has occurred within an acceptable period (ISO, 2019). Business continuity planning establishes risk management processes and procedures to prevent interruptions to mission-critical services and re-establish the full functioning of the organisation as quickly and as smoothly as possible (Convery, 2010b). Effective electronic records management plays a big role in ensuring business continuity in an organisation, as records help in decision-making.

Traditional disaster recovery and business continuity methods can be cumbersome and extremely expensive. They require purchasing and maintaining a complete set of hardware that matches a company's business-critical systems, including sufficient storage to house a complete copy of all the records of the organisation (Convery, 2010a). Convery (2010a) further reasons that storing business information in the cloud can facilitate business continuity and disaster recovery strategies while saving costs. Instead of investing money in acquiring hardware to replicate information onto and store it in an off-site location that is only used during an emergency, organisations can use relatively cheap storage capacities of cloud infrastructure providers (Convery, 2010a). Due to the cloud service provider replicating information to prevent outages and server failures, the availability of information is improved in case of disaster, as the information is replicated across various servers (Bassett, 2015).

The study investigated how clients were assured of business continuity and disaster recovery plans by providers. It further, observed what disaster recovery plans existed and were agreed upon by both parties, as well as the presence of disaster recovery clauses in the service level agreements (SLA).

2.4.7 Greater mobility

Cloud computing allows for broad network access. A client can access cloud computing services over the internet, through a browser using multiple devices with internet capabilities, such as computers, mobile phones or tablets. Services are available regardless of the clients' geographic location (Convery, 2010a; Mell & Grance 2011).

Access to records and information from any location via the internet is an advantage for any organisation that has employees who may work from various locations. Access to stored data from any location is a great potential benefit for records management, as records can be accessed, updated and stored from anywhere. This can help eliminate duplication of records and can be an excellent factor when assessing cloud computing's viability for records management, where individuals can collaborate and share documents with one another, despite their geographical location. Kibe (2016) agrees that cloud computing facilitates the realisation of multi-user access to records, thereby enabling ready access to records and real-time collaboration in decision-making and task performance. The study evaluated how organisations deal with access to records anytime and anywhere, and its impact.

2.4.8 Improved security and compliance

Unlike normal organisation internal computing systems, cloud computing can provide superior security due to the provider having increased resources, such as IT expertise, which are dedicated to solving security issues. The service provider can provide greater expertise and experience in information security practices to individual customers (Convery, 2010a). Resources can be dedicated to improving application security processes and improving the network, as security measures will be easier and more cost-effective to put into place on a larger scale. There are defence measures, such as hardening of virtual instances, patch management and virus protection, which can be implemented rapidly over the entire cloud provider's infrastructure. This is done through automation and virtualisation, which enable the fast implementation and replication of security configurations for the service provider (Bassett, 2015). In addition, the cloud service provider can utilise early incident detection mechanisms, which enable them to respond to security incidents and breaches faster (Convery, 2010a). Dedicated security resources from a cloud service provider can be of great benefit to records management, as it prevents the loss of sensitive documents that have been shared within an organisation over the internet.

Carroll et al. (2011) argue that with cloud computing, the client transfers the responsibility for information security to the cloud service provider. However, the client is still responsible for ensuring that the service provider can provide the necessary security as well as the encryption of the data. Unfortunately, by transferring the responsibility of security to the cloud service provider, the client loses some control. This loss of control can affect the organisation's ability to comply with certain standards and guidelines (see section 1.3.2.). This study investigated the security measures in place to avoid security breaches, hacking and unauthorised access, destruction or manipulation.

2.4.9 Long-term preservation

Kibe (2016) argues that the storage of records in the cloud increases their longevity by decreasing wear and tear that are two of the most common causes of records deterioration in a manual system. Additionally, cloud-based services also enhance the integrity of records compared to physical records, which can be lost, amended or damaged easily. Digital records stored in the cloud will stay usable for longer and always available, thus supporting timely decision-making and service delivery

(McLeod & Gormly, 2017). However, Convery (2010a) advices that using cloud services to establish a central digital repository might present challenges for long-term preservation of information. Corrado and Moulaison (2015) argue that backup does not fulfil the requirement of long-term preservation of records, however, maintaining the meaning of the digital object and its content, provenance, authenticity, securing the context of its creation and use is what ensures it.

This study aimed to find out which benefits of cloud computing for records management were being experienced by the selected Namibian organisations utilising cloud computing for records management. Organisations are at least expected to secure some, if not all, the common potential benefits of cloud computing to ensure cloud computing is a solution for issues associated with the management of electronic records. These benefits, however, should be weighed against the risks associated with the privacy and security of records.

2.5 Risks and mitigating factors of managing records in the cloud

Despite the benefits of cloud computing, storage and maintenance of records with cloud computing service providers have a variety business and legal risks. A study by Chitauro (2017) found that uptime, security of data, privacy and latency requirements were indicated as current concerns in Namibian tertiary institutions. Government of South Australia, State Records of South Australia (2015) urges organisations to do a thorough risk assessment before entering arrangements or contracts with cloud service providers. Moreover, Carroll et al. (2011) agree that although there are many drivers for adopting cloud computing, it is not a completely secure solution without risks. A comprehensive understanding and the moderation of security risks is an important step towards securing cloud environments and harnessing the benefits of cloud computing (Kibe, 2016). Several scholars (Kibe, 2016; Carroll et al., 2011; Convery 2010a, 2010b; Stuart & Bromage, 2010; Mosweu et al., 2019) have indicated that security remains the biggest concern to organisations using or planning to adopt cloud computing for records management.

Organisations are still responsible for the management of their records despite their storage location. Records should be authentic, reliable, and usable and possess integrity as stressed by ISO 15489-1 (ISO, 2016) despite being stored and maintained in the cloud. Stuart and Bromage (2010) argue that the backbone of minimising record management risks in the cloud is for organisations to introduce policies and codes of practice surrounding the use of cloud computing, formulated through consultation between records management and IT units. These policies should focus on user behaviours and address issues like legislative and standards, information confidentiality, integrity and access to information. For this study, the following risks and their mitigating measures were identified as important for records management in the cloud.

2.5.1 Location, legal jurisdiction and compliance

The act of storing records outside a state, territory or country might be a breach of national/local laws (O’Keeffe, n.d.). Some countries may state in policies or acts that the records of their governments must only be stored and maintained within the country. This study sought to identify any such legal restrictions in Namibia. The above risk, if not taken into consideration, may result in providers failing to comply with legislation and standards of the record-creating jurisdiction. The cloud computing and records management guidelines of Australia emphasise that there is a risk when providers store an organisation’s records outside of the creators’ boundaries, that they might fail to comply with the creators’ legislative requirements and that legislative requirements of other states might be applied to those records (Government of South

Australia, State Records of South Australia, 2015). The Government of South Australia further explains that it is possible for privacy laws of an overseas jurisdiction to be applied to information stored within the jurisdiction despite its originality, which might permit access to your information by investigative or regulatory bodies within the jurisdiction where the information is stored.

Carroll et al. (2011) argue that organisations comply with requirements, acts and regulations set by their own organisation or by an industry or government body, for securing both internal and external data and applications. Cloud computing, in most instances, means data and applications are hosted at an off-site location, outside the legal and regulatory framework of the organisation. However, compliance needs to be proved regardless of the location of data (Mosweu et al., 2019).

Mosweu et al. (2019) further argue that to avoid risks associated with location, legal jurisdiction and compliance, organisations need to ensure that the cloud service provider is willing to undergo external audits and security certifications, and that logs ensuring compliance are readily available. In addition, the client should clearly indicate in the SLA the geographical locations permitted for their records and cloud service providers should prove that data, including all copies and back-ups, are stored only in geographic locations permitted in the agreement (Carroll et al., 2011). Convery (2010a) claims that cloud computing presents records management with new complexity to legal and regulatory compliance because existing laws and standards were not established to accommodate cloud computing. Organisations need to revise and find a way to adopt existing procedures to meet cloud computing security challenges. Adhering to access legislation and other regulations such as the Data Protection Act and Freedom of Information Act, organisations need to know the type of records held in the cloud, where it is held and how it can be accessed (Mosweu et al., 2019).

Convery (2010a) opines that for organisations to avoid non-compliance with relevant legislations, assessment of how storing records in the cloud can affect legal and regulatory compliance need to be done, as well as how processes to ensure continued compliance can be established. In addition, third-party audits should be performed regularly to monitor the cloud service provider's compliance to agreed terms to ensure adherence to standards, procedures and policies, as well as that no major changes occurred to any of the standards, procedures or policies as per the agreement with the client (Carroll et al., 2011).

This study aimed to find out how issues of compliance were addressed by both cloud providers and clients. Moreover, the study investigated the existence of policy and regulation documents needed to ensure compliance.

2.5.2 Authenticity, reliability, integrity and accessibility of records

Authenticity, reliability, integrity and accessibility are the four characteristics of trustworthy electronic records. Electronic records lack physical and visual clues about their origins and their authenticity. An authentic record is one that can be proven to be what it purports to be; reliability is when a record can be trusted as a full and accurate representation of transactions; integrity means the record is complete and unaltered; while accessibility refers to the ability of locating, retrieving, presenting and interpreting an electronic record (State Archives of North Carolina, 2013). IRMT (1999b) elaborates that managing electronic records can be challenging since they are easily revised, deleted, changed and manipulated. Maintaining the attributes of electronic records (content, structure and context), therefore, is both more vital and difficult than with traditional paper records. Cautious planning and system design are required to guarantee that the attributes of electronic records are captured and maintained for the lifetime of the record. Content refers to the information in the record (such as numbers, text, symbols, images or sound); structure refers to the appearance and arrangement of the content (such as file format, data organisation, page layout, style, and fonts); and context refers to information that shows how the record is related to the business of the agency and other records, such as title, author, time, purpose and transaction (IRMT, 1999b). Metadata, simply defined as "data about data", can provide a key to understanding the origins, authenticity, purposes, and uses of electronic records. Because it is so easy to change and disseminate electronic records, guidelines must be put in place to ensure that they retain authenticity, accuracy, integrity, and accessibility (Stuart & Bromage, 2010).

Stuart and Bromage (2010) proclaim that although there are significant benefits to leveraging cloud computing, security concerns lead organisations to hesitate to move critical information to the cloud. The integrity of data in complex cloud hosting environments could provide a threat against data integrity if system resources are not effectively separated among customers (Carroll et al., 2011). Convery (2010a) points out that data integrity is assured when data is consistent and correct and only changes in response to authorised transactions. Another risk in cloud computing environments is unauthorised changes to data and systems by the service provider, which could affect the integrity and availability of data and applications (Carroll et al., 2011).

Convery (2010a) further endorses that the authenticity, reliability, integrity and accessibility of records rests on the ability to demonstrate that the record has not been manipulated or tampered with. Records characteristics are at risk of being compromised in the cloud by:

- unauthorised access by malicious insiders at the cloud provider,

- interception while in transfer over an unsecured network, and
- Being mixed up with records of other clients in a multi-tenant environment.

Cloud-based services result in mobile users accessing records from wherever they are, leaving an organisation's records open to large threats. Carroll et al. (2011) uphold that hackers no longer need to come on premises to steal data, and they can find it all at once through virtual locations. Thus, security measures need to be put in place to protect the features and characteristics of records for their evidential value.

Furthermore, there could be a risk of loss of control over information stored in the cloud. This is a concern that has implications on the ability to manage the information life cycle, information security and authenticity (Kibe, 2016). Carroll et al. (2011) elaborate that the ability to achieve information life-cycle management, such as access, classification and retention, in the cloud depends on the cloud provider system's functionality and the kind of information that is stored in the cloud, for example, inactive records with their retention periods can be deleted easier. Responsibilities for infrastructure, and thus information security, are to varying extents transferred to the cloud services' provider (depending on the service model), and need to be established from inception (Convery, 2010b). Convery further argues that the ability to monitor and audit the cloud provider's systems is frequently limited as cloud providers aim to keep details of their infrastructure and security processes secret from the competitors and hackers. Carroll et al. (2011) remark that failure to obtain access logs and incident reports from cloud providers can have an impact on the evidential value of information stored in the cloud for legal and compliance requirements. Carroll et al. (2011) further allege that lack of standards and audit procedures makes it difficult for an organisation to obtain the relevant information to satisfy their compliance and 'due diligence' requirements.

Organisations transfer many of the responsibilities for keeping their record secure in the cloud to the providers. To maintain the characteristics of electronic records in the cloud, a client should exercise due diligence when selecting a cloud provider. The provider should be able to answer questions regarding functionality, reliability, usability, authenticity, security, data ownership, integration and customisation (Government of South Australia, State Records of South Australia, 2015). However, it is the client's responsibility to make sure that the provider has the necessary information security procedures in place. The integrity, authenticity, reliability and usability of records rests on the ability to prove that the records have not been manipulated or tempered with over time either by unauthorised access, unsecure network, or mixed up with other client's records (Convery, 2010a).

Carroll et al. (2011) state that records should be properly identified and classified to point out those that are too sensitive to be managed in the cloud. Additionally, the cloud service provider's security and information personnel must have adequate knowledge and skills to prevent, detect and react to security breaches in a timely fashion. Moreover, third-party audits should be performed regularly to monitor the provider's compliance to agreed terms, and the effective implementation of and adherence to security policies, procedures and standards set by the client.

Carroll et al. (2011) further argue that to prevent unauthorised changes to records by cloud providers, all changes in the cloud environment should be managed to minimise the likelihood of disruption, unauthorised changes or errors by developing and implanting standards and policies to guide developers during development and restricting users to authorised data. Besides, service providers have a duty to keep auditable proof that no unauthorised changes occurred during a specified period and should be transparent with their clients (Council of Australian Archives and Records Authorities, 2010).

2.5.3 Retrieval and disposal of records

Retrieval and disposal of information presents a series of challenges relating to how information can be identified, searched and destroyed in the cloud (Kibe, 2016). There is a need for a mechanism to classify, label or search for records in the cloud to enable their retrieval when needed. Convery (2010b) argues that the ability to apply classification schemes through metadata depends on the cloud provider's systems and programmes. Similarly, it needs to be established in which format information can be transferred and used in the cloud provider's systems and applications to avoid the change of information formats during transfer as this might impact the organisation's ability to prove the information's authenticity (Convery, 2010a).

Moreover, information retrieval can be difficult, time consuming, and costly, if the cloud provider does not offer standard mechanisms for information retrieval. Ransome and Rittinghouse (2010) concur that records retrieval can also be lost once a cloud computing service or contract is terminated without an exit strategy for the retrieval or destruction of the information. The transfer of information between different cloud providers can be difficult as cloud providers use proprietary Application Programming Interface (API) and interoperability is widely lacking (Kibe, 2016).

The implementation of retention decisions in the cloud can be difficult to achieve, if the cloud provider does not offer retention management functionality (Convery, 2010b). In agreement, Kibe (2016) states that records in the cloud may be saved using the services from several service providers, hence, creating a challenge when establishing how long a record can be retained in an organisation. Kibe (2016) further stresses the need to sign a memorandum with the service provider to safeguard their role in determining records-retention requirements. Moreover, most cloud providers will delete nodes pointing to records, hiding them from the virtual server. However, this does not mean the records are totally wiped out from the hard drives, leaving potential room for the records to be accessed by a third-party who can access the provider's infrastructure (Carroll et al., 2011). Correspondingly, Kibe (2016) affirms that lack of capabilities to implement records disposal schedules results in organisations facing challenges when attempting to delete records permanently or transferring them to the archives due to the wide range of storage options offered by providers that can be used to revive records against the will of the organisation.

Furthermore, reliance on the internet as the primary medium of data transfer and processing leads to availability issues due to possible connectivity and bandwidth speed limitations (Convery, 2010b).

The main reason for managing records in an effective manner is to be able to retrieve them for proper business operation and to provide evidence of business transactions. There are concerns to how records can be identified, searched and destroyed once they are managed in the cloud. Convery (2010b) argues that the ability to apply classification schemes through metadata by the cloud services highly needs to be established to facilitate effective retrieval. The study investigated how classification schemes and retention schedules were applied to records in the cloud.

Records need to be available and back-up and recovery schemes for the cloud must be in place and effective to prevent data loss, unwanted data overwrite, or destruction. Organisations using cloud services should ensure that cloud providers have adequate back-up and data replication policies and should keep auditable proof of the adequacy of restore procedures including accurate, complete and timely recovery of data (Carroll et al., 2011).

Furthermore, internet connectivity and bandwidth speed limitations should be investigated before considering moving records into the cloud, as well as guiding the selection of a suitable service provider. Network services and management should provide for adequate provisioning of bandwidth speed and network capabilities (Ferguson-Boucher, 2011).

It is the client's responsibility to ensure and establish if the provider offers retention management functionalities in the cloud services offered. It must be clear that when records are deleted due to their retention period, they are wiped off all the providers' hard drives and not simply overwritten, which could enable a third party to access them (Convery, 2010b).

At the implementation stage, an organisation must ensure that an exit strategy is in place to outline the retrieval or disposal of records from the cloud once a contract is terminated (Convery, 2010b). In the absence of such an exit strategy, records retrieval can be difficult, time consuming and costly. Concisely, the client must ensure that the provider has the right processes in place to destroy records when requested.

2.5.4 Security of records in the cloud

Cloud computing for records management may present risks of unauthorised access to records, which will result in breaches to privacy laws. Unauthorised access to records may happen due to poor security controls or co-locating multiple clients' records. Furthermore, there might be loss of access to records on some occasions due to poor internet connectivity, which will affect continuous access to records that are needed for business activities (McLeod & Gormly, 2017). Additionally, records can be lost due to cyber-attacks, provider gone out of business, provider's organisation taken over by another organisation or inadequate backup and restoration arrangements (Government of South Australia, State Records of South Australia, 2015).

Stuart and Bromage (2010) claim that fragile authentication mechanisms could increase the risk of unauthorised access to data and applications, which are globally accessible through the cloud and being shared with other customers due to the multi-tenancy nature of, cloud computing. Weak authentication mechanisms may include insecure user behaviour (that is, weak passwords or re-using of passwords), the inherent limitation of one-factor authentication mechanisms and inadequate segregation of duties (Stuart & Bromage, 2010). Migrating workloads to shared infrastructure leads to potential unauthorised access and exposure, including challenges such as credential management, strong authentication (that is, multi-factor authentication), delegated authentication and managing trust across all types of cloud service (McLeod & Gormly, 2017).

Security challenges top the list of risks to records management in the cloud. Compared to other digital records that may have risks such as destruction by disasters like fire or cyber-attacks, records in a cloud computing environment have additional risks outlined by Government of South Australia, State Records of South Australia (2015) as:

- An organisation in another country accessing, claiming ownership or taking control of your records;
- Records not being returned upon request or at the end of a contract, or large payments requested for records return;
- Inadequate backup and restoration arrangements due to cost cutting by the provider;
- Provider upgrading to hardware and or software that is not compatible with that of your agency, risking data loss or inaccessibility or unreadable formats, and
- Provider disposing of digital records without client permission.

Studies on cloud computing and records management found other risks and challenges in managing records in the cloud (Kibe, 2016; Mosweu et al., 2019; Asogwa 2012; Mosweu 2012; Ngoepe & Saurombe, 2016):

1. Poor retention and disposal capabilities – due to the replication of information in the cloud, clients do not have assurance of permanent deletion of all replicas of a record at disposal.
2. Trustworthiness and sustainability of records – This arises because most cloud platforms available do not have practical standards governing how records are stored and manipulated. The unreliable nature of cloud computing brings about doubts whether all attributes of electronic records (content, structure and context) are preserved to maintain authenticity, accuracy, integrity and accessibility.
3. Security of records is compromised in the cloud – organisations do not have control or knowledge of where their records are stored. This means such records will remain vulnerable to malicious manipulation.
4. Long-term preservation – cloud providers fail to demonstrate strategies for continuity of records with permanent value.

Like any other records, records stored and maintained in a cloud environment need to be managed in such a way that they can be proven to be authentic, reliable and accessible and thus the evidential value of records need to be protected (Stuart & Bromage, 2010). However, in a cloud environment evidential value of records may be damaged if audit trails and descriptions of management processes performed on records are not maintained.

Organisations handover the responsibilities for records security to cloud providers when they manage their records in the cloud. The loss of control over the security of and access to records highly depends on the selected cloud service model, that is, IaaS, SaaS or PaaS. To minimise the risk of unauthorised access, loss of access and unauthorised destruction of records, the cloud provider must be able to demonstrate the existence of effective and robust security controls, assuring customers that data and applications are adequately secured against unauthorised access, change and destruction (Convery, 2010a).

Carroll et al. (2011) argue that consistent reviewing and monitoring of privileged access should be performed, including who manages and administers data and the adequacy of such rights, proper separation of duties, the handling and disclosure of changes in system controls and access restrictions, and controls and formal procedures to prevent, detect and react to security breaches. Moreover, Carroll et al. (2011) state that the client needs to enquire on the competence of the service provider's hiring and management process for administrators and those responsible for management and monitoring of cloud computing services to establish their knowledge in security requirements for records. Thus due diligence is an important consideration when choosing a cloud computing service, deployment model and provider. The study investigated the records management expertise of staff involved in deploying cloud computing services.

Convery (2010b) affirms that cloud service providers ought to ensure that all access or changes to cloud services, resources and data produce auditable records regardless of success or failure. Audit trails should include clear indications of any delegations of identity or authorisations. Convery (2010a) further affirms that to ensure high-level security there is a need for adequate authentication, identity management and compliance, and access security tools and techniques should be implemented and regularly monitored for compliance. There is also a need to ensure that a high degree of transparency to the service provider's operations is negotiated and documented in the SLA and formally agreed upon by both parties. The study probed whether there were written agreements in place between the cloud service providers and the clients. The Australian Digital Recordkeeping Initiative (DRI) issued a ‘recordkeeping checklist for government agencies considering using cloud computing service providers’, which can be used by any other agency to minimise records management risks in cloud computing (Council of Australian Archives and Records Authorities, 2010).

2.6 Summary

This chapter discussed literature on the use of cloud computing for records management. The literature revealed that cloud computing presents both benefits and risks to records management. Cost-efficiency, business continuity, greater mobility, availability and reliability, modernisation of business processes and scalability are some of the potential benefits cloud computing offers for records management. Despite the benefits of cloud computing, it also presents risks for the organisation, such as location and jurisdiction compliance, difficult retrieval and disposal. Security remains the major risk in managing records in the cloud, with concerns of loss of records and unauthorised access or destruction. However, there are factors to consider when deciding to adopt cloud computing that mitigate those risks. Applying due diligence during the selection of service models, deployment models and a cloud provider is the backbone of mitigating records management risks stored in the cloud.

Many organisations have started to use cloud-based services for records management. This is because of the potential benefits of cloud computing. These benefits, however, should be weighed against the risks associated with the privacy and security of records, because the records migrated to cloud spaces should retain their reliability, authenticity and integrity. They should also continue to be usable, and, when necessary, securely destroyed or transferred. Consequently, organisations moving records to cloud spaces should develop mandatory policies to regulate the use and protection of their records. Moreover, the literature revealed that the few studies conducted on cloud computing in Namibia are on technical aspects of cloud computing. This study applied cloud computing services and deployment models as the conceptual framework. The success of cloud computing for records management highly depends on the type of service and deployment model adopted. The next chapter discusses the research methodology.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides an overview of the research methodology of the study, which focused on assessing the use of cloud computing for records management in selected organisations in Namibia. Research methodology describes what was done to attain research objectives and how the research was done (Bless et al., 2013). In addition, it explains how the results were analysed and gives full details on how the researcher was able to come up with the solution to the problem statement (Neuman, 2014). Leedy and Ormrod (2013) describe research as a systematic procedure of gathering, analysing and interpreting information in order to increase the understanding of a phenomenon about which concerns us. Moreover, the chapter discusses the research design, data collection methods, the population, sampling methods, sample size, research instruments, reliability and validity, procedures and data analysis. It further presents the research ethics and evaluation of the research methodology. Finally, the summary of the chapter is provided.

3.2 Philosophical Assumptions

Philosophical assumptions are a set of general beliefs or assumptions that direct and inform research studies (Creswell & Plano Clark, 2011). Research paradigms address three main assumptions: ontology, epistemology, and axiology (Creswell, 2003). A researcher chooses a stance on each of these assumptions, and the choice has practical implications for designing and conducting research.

Ontology refers to the nature of reality and the fact that reality is subjective and multiple as seen by participants of a study (Creswell, 2007). When researchers conduct qualitative research, they are embracing the idea of multiple realities. Different researchers and research participants embrace different realities. Creswell (2007) further argues that researchers reports these different realities using multiple quotes and themes in words of participants and provides evidence of different perspectives.

Epistemological assumptions mean that researchers try to get as close as possible to the participants being studied, by conducting the study where the participants live and work (Creswell, 2007). The study of these participants' experiences could only be captured by hearing what they have to say since they are the ones who lived through the process. In this multiple case study, the researcher focused on the participants and listened to their views and experiences regarding the use of cloud computing for managing records.

The axiological assumption that characterises qualitative research is that all researchers bring value to a study, but qualitative researchers like to make explicit those values (Creswell, 2007). In a qualitative study, the inquirers admit the value-laden nature of the study and actively report their values and biases as well as the value-laden nature of information gathered from the field (Creswell, 2007). The researcher was cognisant of this and attempted to address them through ethical considerations and style of interviewing. The types of questions asked were influenced by the researchers' worldviews. The analysis of the findings and depiction of themes were also influenced by the researchers' values, personal experiences, and worldviews. At the same time, the values, experiences, and worldviews of the participants interacted with those of the researchers to deepen the analysis.

This study preferred qualitative research as opposed to quantitative research due to the flexibility of this approach, which best answer the research questions in situations where little is known about the topic (Bricki & Green, 2007), as was the case with assessing the use of cloud computing for records management in Namibia.

Qualitative research focuses on understanding humans from multiple perspectives (Burton, 2000). Creswell (2007) emphasised that in qualitative research, a researcher collects data in a natural setting delicate to the people and place under study in order to understand how individuals or groups ascribe to the research problems. In this study, the researcher collected data at the premises of three organisations to gather their aspects in their natural environment and interviews for the fourth organisation were conducted virtually due to the Covid-19 pandemic.

3.3 Research Design

Durrheim (2006, p. 34) defines research design as a "strategic framework for action that serves as a bridge between research questions and the execution or implementation of the research". Research design is also defined as everything involved in planning and completing a research project, from identifying the problem up to reporting and publishing the results (Punch, 2005). According to Durrheim (2006), a researcher needs to make a series of decisions along dimensions of purpose of the research, the conceptual paradigm informing the research, the context within which the research is carried out as well as the research techniques employed to collect and analyse data in order to maximise the validity of the findings.

The study adopted a multiple case study research design. It comprised of four cases, which are private organisations in Namibia. Three organisations were cloud computing providers and one was a cloud computing client. In multiple case study research design, a researcher explores multiple cases through in-depth data collection methods, that is, interviews, observations, documents and reports (Yin, 2009; Creswell, 2007; Patton, 2015). Yin (2009) suggests that multiple case study design uses the logic of replication, in which the researcher replicates the procedures for each case to establish the similarities and differences between the cases. This research replicated the procedures and methods for all four cases during data collection. Yin further argues that results generated from multiple cases are far more convincing and robust compared to single case results.

3.4 Data Collection Method

This section discusses the data collection method that was used to collect the data for this study. Qualitative researchers study spoken, observed and written representations of human experience, via multiple methods and multiple data sources (Punch, 2005). The choice of method of data collection is often based on its appropriateness in answering the areas of investigation in a study. This study used semi-structured interviews to collect data.

3.4.1 Interviews

Interviews are a major data collection instrument in qualitative research, which presents a good way of accessing people's perceptions, meanings, definitions of situations and constructions of reality (Punch, 2005). Interviews can be structured, unstructured or semi-structured. Structured interviews are verbally administered questionnaires with a list of predetermined questions, while an unstructured interview is a conversation with little or no order (Thomas, 2011; Punch, 2005).

This study used semi-structured face-to-face interviews to collect data from the IT and records management staff at the private organisations. Semi-structured interviews enable both the researcher and respondent to be flexible and diverge to pursue an idea or detailed response (Thomas, 2011). This interview format is useful for qualitative case study research, as it provides participants with guidance on what to talk about, which helps with data analysis and interpretation (Punch, 2005). Gill et al. (2008) argue that the flexibility of this approach compared to structured interviews, allows for the discovery or elaboration of information that is important to participants but may not have previously been thought of as pertinent by the researcher.

The interviews were beneficial to this study because they presented the researcher with an opportunity to elaborate on the questions, which enabled the participants to give clear and concise responses. Interviews can be conducted in-person or virtually. This study's interviews were conducted in-person for some respondents and virtually for others.

3.5 Population

A study population is the total number of possible units, elements or cases that could be included in the study (Gray, 2009; David & Sutton, 2011). Simplified, a population of a study is the entity that the researcher bases a study on. David and Sutton (2011) state that a population‘s units of analysis may be characterised in terms of individuals, groups, organisations or documents usually defined by the research questions and/or objectives. Gray (2009) defines units of analysis as individuals, organisations, groups and data series – they are the objects of the study.

The population of the study was Namibian private organisations providing and/or utilising cloud computing for records management.

3.6 Sample

Durrheim (2006, p. 49) defines sampling as "the selection of research participants from an entire population, and involves decisions about which people, settings, events, behaviours, and/or social processes to observe". Bless et al. (2013) opine that a sample is the subset of the whole population that a researcher is investigating and whose characteristics will be generalised to the entire population. The aim of sampling is to select a sample representative of the whole population under study (David & Sutton, 2011). However, Durrheim (2006) argues that qualitative research is less concerned about statistical accuracy of representation and more concerned with detailed and in-depth analysis, thus typically large random samples are not necessary. Nengomasha (2009) agrees that qualitative research uses relatively smaller samples compared to quantitative studies. In agreement, Patton (2015, p. 310) states that there are no rules for sample size in a qualitative inquiry. According to Patton's argument, sample size depends on what you want to know, the purpose of the inquiry, what is at stake, what will be useful, what will have credibility, and what can be done with the available time and resources.

The most suitable sampling technique for this study was the non-probability sampling using the purposive method. Non-probability sampling chooses subjects to be part of a sample in non-random ways. Purposive sampling, also known as judgemental, selective or subjective sampling, is a type of non-probability sampling technique where the units are selected based on the knowledge, good judgement and opinion of the researcher (David & Sutton, 2011; Punch, 2005; Leedy & Ormrod, 2010). According to Patton (2015), the strength of purposive sampling lies in selecting information-rich cases that offer in-depth understanding of the phenomena under study.

This study assessed four private organisations in Namibia that provided and/or were utilising cloud computing for records management and were willing to partake in the study. A research paper done by Chitauro (2017) identified five cloud service providers in Namibia. This study aimed at generalising its findings to the Namibian private sector. According to Creswell and Poth (2018), to best generalise, the researcher needs to choose representative cases for inclusion in a qualitative study. Silverman (2000) argues that generalisability is a customary aim in quantitative research achieved by statistical sampling procedures, which are usually not a norm in qualitative research. Generalisability in case study research has been particularly negatively criticised. However, Punch (2005) states that a case study can yield generalisable results, depending on the purpose of the study and its data analysis techniques.

The selection of participants within the four selected private organisations was done purposively. The researcher selected three categories of participants: IT staff from a cloud computing provider, IT staff from a cloud computing client and records management staff from the cloud computing client. The three categories of participants were all selected purposively due to their direct involvement with cloud computing and records management. The study aimed at sampling from each organisation at least two respondents from the IT staff categories of both the cloud provider and the cloud client and two respondents from the records management staff category. The study found that organisations employed very few staff in the two units of IT and records management. As a result, the study ended up with a small sample of seven participants: five IT staff and one records management staff from cloud computing providers, and an administration staff member from the cloud computing client organisation.

3.7 Research Instrument

This section discusses the research instrument used by this study, which can be simply referred to as a tool used to gather or collect data for a study. This qualitative study used semi-structured interview guides.

The semi-structured interview guides are discussed in detail below:

3.7.1 Interview guides

An interview guide is a list of topics, themes, or areas to be covered during an interview, prepared in advance by the researcher to allow flexibility in the topics and areas to be covered (Lewis-Beck, Bryman & Liao 2004). Interview guides, as explained by Patton (2015), further aided the researcher with carefully using limited time, ensuring the interviewing of the respondents is systematic and comprehensive and keeping interactions focused while still allowing perspectives and experiences to emerge. There are three types of interview guides: unstructured, semi-structured and structured (Thomas, 2011). This study opted for semi-structured interview guides that helped the researcher maintain a systematic structure, while offering flexibility to the study to seek more details from respondents (Punch, 2005). Semi-structured interview guides were further preferred for this study, as the researcher carried out the interviews personally to enable probing during the interviews.

This study used three sets of semi-structured interview guides: one for IT staff of the cloud computing provider (see Appendix D), another one for IT staff of the cloud computing client (see Appendix E), and one for records management staff (see Appendix F).

When designing an interview guide, it is imperative to ask questions that are likely to yield as much information about the study phenomenon as possible and can address the aims and objectives of the research (Lewis-Beck et al., 2004). The interview guides addressed the following areas of the study, guided and linked to the study objectives:

- Reasons for adopting cloud computing for records management.
- Cloud computing services and deployment models.
- Factors to consider when choosing a cloud service provider, service and deployment model(s).
- The benefits of cloud computing for records management.
- Risks of managing records in the cloud.
- Measures to mitigate risks of managing records in the cloud.

3.8 Reliability and Validity

According to Silverman (2000, p. 175) “unless you can show your audience the procedures you used to ensure that your methods were reliable and your conclusions valid, there is little point in aiming to conclude research”. Reliability is concerned with the accuracy of the actual measuring instrument or procedure, while validity is concerned with the study's success at measuring what the researchers established to measure (Creswell, 2007; Silverman, 2000; Punch, 2005). Qualitative research, especially case studies, receive a great deal of criticism in establishing reliability and validity since these concepts are traditionally applicable to experimental and quantitative research (Farguhar, 2012; Liamputtong & Ezzy, 2005). Nieuwenhuis and Smit (2012) oppose the use of the terms reliability and validity for qualitative research and suggest credible and trustworthy as more suitable. This section discusses how the study ensured credibility and trustworthiness.

To maximise credibility and trustworthiness of the findings, the study used data verification by deliberately seeking evidence from more than one case and more than one staff category, and comparing the findings from those different cases (Patton, 2002). The study collected data from different organisations using the same interview guides, establishing a comparison case and seeking out similarities and differences across accounts to ensure different perspectives were represented.

3.9 Data Collection Procedures

Research procedure can be defined as the order or manner that one follows before or during the gathering of data. The procedure followed by the researcher entailed obtaining research permission from the University of Namibia (UNAM) (see Appendix E) that was used to seek authorisation to collect data in the organisations. The organisations gave permission for the study to be carried out and internally informed their staff with whom the researcher set interview appointments via email and telephonic conversations.

Before the commencement of interviews, participants signed informed consent forms and each interview took approximately 45 minutes. The researcher carried out all the interviews personally, some face to face and others virtually using of interview guides while recording and noting down the responses with the permission of the interviewees.

3.10 Data Analysis

Analysis of data entails inspecting, cleaning, transforming, and modelling data with the goal of discovering useful information, suggesting conclusions, and supporting decision-making (Patton, 2002). According to Creswell (20017, p. 37), "the final written report or presentation includes the voices of participants, the reflexivity of the researcher, and a complex description and interpretation of the problem and it extends the literature or indicates a call for action". This study opted for the content analysis technique.

Content analysis involves making inferences about data by systematically, and objectively identifying special classes or categories within the data (Gray, 2009). Miles and Huberman (1994) claim that content analysis involves three activities: data reduction, data display and conclusion drawing and verification. These activities are to sort, focus, organise and interpret data for conclusions to be drawn and verified (Gray, 2009; Creswell & Poth, 2018). Good analysis depends on understanding the data, for qualitative analysis, this means going through the data repeatedly and breaking it down (categorising). Content analysis is for all types of recorded data, including interview notes, observation notes and audio recordings (Blanche, Durrheim

& Kelly, 2006). This study analysed handwritten notes and audio recordings obtained during semi-structured interviews.

The researcher analysed data by going through raw data repeatedly to break it down into categories, those linked to the study objectives and those that emerged from the data analysis process (Blanche et al., 2016; Patton, 2015). Categorising in qualitative analysis means identifying themes or patterns, ideas, concepts, behaviours, interactions, incidents, terminology or phrases used and organising them into coherent categories that summarise and bring meaning to the data (Tylor-Powell & Renner, 2003). Themes and categories were then interpreted considering their connections to the study objectives to explain the findings of the study.

3.11 Research Ethics

Research ethics are concerned with the appropriateness of the researcher's behaviour in relation to the participants of the study and those affected by it (Gray, 2009). Ethics are an important aspect of research. According to Wassenaar (2006), research ethics seek to ensure that the welfare of research participants is protected. Since social research deals with people and issues that affect them, ethical issues can arise at the planning, implementation and reporting phases of research (Gray, 2009). This study involved human participants and it was mandatory to apply for ethical clearance from the UNAM Research Ethics Committee before collecting data. (See Appendix G for the ethical clearance approval).

There are various principles of ethics this study considered and these are autonomy, beneficence, anonymity and confidentiality (Wassenaar, 2006). Autonomy is concerned with respect for the participants and their decision to be part of the study or not. It is the researcher's responsibility to provide the respondents with sufficient information about the study for them to make informed decisions on whether they are willing to be involved (Gray, 2009; Wassenaar, 2006). At the beginning of the study, the purpose of the study was explained to the respondents to ensure that they understood the research and its benefits thereof. The participants were provided with an informed consent form (see Appendix H) to read and agreed to be part of the research by signing it. However, they were also given an option to withdraw without any adverse consequences. Beneficence obliges the researcher to attempt to maximise the benefits of the research to participants. Wassenaar (2006) argues that these benefits do not include payment to the participants, but must be more direct such as knowledge gained. This principle was achieved by sharing the findings of the study with the participants and their organisations. Anonymity and confidentiality are considered an essential concern for research participants. In this study, coding respondents and organisations ensured confidentiality by not mentioning their names in reporting the findings.

Moreover, other ethical issues such as tape recording during the interview were dealt with by requesting permission from participants. Participants who did not permit recording were given the option to participate without recording. The researcher truthfully recorded what the participants provided without including personal opinions. Data collected for this study is virtual and will be stored on Google drive for five years.

3.12 Evaluation of the research methodology

This section evaluates the research methodology used for this study. Evaluation of methodology helps readers and future researchers to discover the strengths and weaknesses of the methods used, which could inform their decisions in case of replication of the study (Nengomasha, 2009). Several authors of research design acknowledged that there is no research methodology without limitations; each methodology has some drawbacks (Gray, 2009; Punch, 2005; Blanche et al., 2006; Creswell & Poth, 2018). This multi-case study employed the qualitative research approach.

The researcher aimed at triangulating data collection methods. However, it was not possible as the researcher was denied access to documents due to confidentiality agreements between cloud providers and clients. According to Creswell (2014), not having "enough information to present an in-depth picture of the case limits the value of some case studies" (p.102). This study was a case study, thus, it was more suitable to use the qualitative research approach to gain a complex, detailed understanding of the topic understudy. Moreover, in circumstances where little is known, it is better to start with qualitative methods, which will help with generating hypotheses that can then be tested by quantitative methods (Bricki & Green, 2007; Gray, 2009). As stated earlier, little research has been done on cloud computing and records management in Namibia.

Due to the Covid-19 pandemic, the researcher experienced a delay in making interview appointments and conducting interviews, resulting in the use of Zoom video conferencing to collect data from some of the participants. If this research were to be conducted again, the use of triangulation method and the use of both qualitative and quantitative methods could be considered to maximise findings.

3.13 Summary

This chapter provided a detailed discussion of the research methodology employed by this study. The study took the interpretivist paradigm and followed the qualitative research approach in the form of a case study design. The data collection method used was semi-structured interviews. The population of the study was Namibian private organisations providing or/and utilising cloud computing for records management and a sample of seven participants was selected from four organisations following the nonprobability sampling using the purposive method. Participants included IT and records management personnel. Permission to conduct research was sought and granted by the organisations. Data was analysed through content analysis and ethical issues were addressed including the use of consent forms.

The next chapter analyses and presents the data.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION

4.1 Introduction

According to Patton (2002), analysis of data involves inspecting, cleaning, transforming, and modelling data with the goal of discovering useful information. This chapter analyses and presents the research data collected through interviews in four private organisations in Namibia. The data were analysed using content analysis, which according to Gray (2009), involves making inferences about data by systematically identifying special categories within data. Anonymity and confidentiality are an essential concern for research participants (Wassenaar, 2006). To maintain confidentiality, names of organisations and participants have been withheld. Organisations and participants are distinguished by codes where it is necessary to specify a particular organisation or participant. Data is mainly presented in the form of descriptive narrative with direct quotes from participants. Data from the different organisations and interview categories have been integrated and incorporated into coherent categories.

This chapter's layout is according to the following study objectives categories and other themes that emerged from the content analysis are presented under the objective they address:

- ▪ Analyse the cloud computing services and deployment models adopted by the selected Namibian organisations:
- Awareness of records management and cloud computing
- Records management expertise for cloud computing
- Cloud service(s) and deployment model(s) provided for records management
- Choosing a cloud service(s) and deployment model(s)

- Assess the factors which drove the selected Namibian organisations to adopt cloud computing are related to records management:
- Cost of cloud computing for records management
- Integration of legacy systems into cloud computing
- Benefits of adopting cloud computing for records management
- Improved staff productivity
- Disaster recovery and business continuity
- Competitive edge
- Assess the risks of managing records in the cloud experienced by the selected Namibian organisation:
- Legislative and regulatory security risks
- Employees' security responsibilities
- Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations:
- Controlled access
- Cultivate awareness
- Security shared responsibility
- Audit trails

Data were collected through three semi-structured interview guides, that is, one each for IT staff of cloud computing provider, IT staff of cloud computing client, and records management staff. These guides were designed to address the study objectives from different angles. The guide for IT staff addressed the above issues from a technical perspective of cloud computing solutions, whereas the guide for records management staff addressed the above issues from an electronic records management perspective. The study intended to collect data through direct observation, however, the researcher was unable to do so due to participating organisations' contractual agreements. Therefore, the data presented and analysed were collected from interviews only.

4.2 Response Rate

The researcher intended to collect data from cloud computing providing organisations and cloud computing client organisations to assess the use of cloud computing for records management from a balanced perspective. However, only one cloud computing client organisation was willing to participate in the study. To get a full view of the usage of cloud computing for records management, the study had intended to interview at least two respondents from the IT staff categories of both the cloud provider and the cloud client and two respondents from the records management staff categories of both cloud provider and client which could have resulted into 16 participants. The study ended up with seven (43%) participants, six from cloud computing services-providing organisations, and one participant from the cloud computing client organisation. The response rate for the study was, therefore, 43%, which is a total of seven people interviewed for this study. The study found that organisations employed very few to no staff in the two units of IT and records management from which the sample was taken. Baruch and Holtom (2008) note that low response rate is expected when a study requires a specific type of target population due to its relevance to the research focus. This was the case with this study which focused on organisations that provided and/or adopted cloud computing services for records management. However, according to Baruch and Holtom (2008), a response rate of 43% is acceptable for studies conducted at the organisational level seeking responses froorganisational representatives. Baruch and Holtom (2008) added that recently published research suggests a benchmark of approximately 35–40% response rate for such studies.

The research participants were from four private organisations, which comprised of three cloud computing providers and one cloud computing client. The participants included IT and records management staff from cloud computing providing organisations and a cloud computing client organisation. However, only one cloud computing provider had a records management personnel on its workforce. The cloud computing client did not have IT or records management personnel dealing with the cloud computing solution adopted. The participant was a human resources consultant acting as a records administrator and mediated between the organisation and the provider. Respondent D1 narrated, "We are a small organisation and we sought for a cloud computing solution to avoid employing IT and information management personnel in order to cut labour costs". The cloud computing services company provided all assistance and training. This finding addresses objective 1.5.2 of the study. Table 4.1 shows the participants with their assigned codes for anonymity, interviewed from four organisations. The participants are divided into two categories: IT staff from cloud computing providers and records management staff (cloud computing provider and client).

Table 4.1: Study participants

(N=7)

Organisation	**Total number of interviewees**	**Number (N) of participants by category and their codes**	
		IT Staff	**Records management staff**
Organisation A Cloud computing service provider	3	N =2 A1 A2	N=1 A3
Organisation B Cloud computing service provider	1	N=1 B1	N=0

Organisation C Cloud computing service provider	2	N=2 C1 C2	N=0
Organisation D Cloud computing service client	1	N=0	N=1 D1

4.3 Presentation of the findings

4.3.1 Analyse the cloud computing services and deployment models adopted by selected Namibian organisations

The first objective of the study sought to analyse the cloud computing services and deployment models adopted by the organisations. The findings to this objective are presented under the following sub-headings:

4.3.1.1 Awareness of records management and cloud computing

4.3.1.2 Records management expertise for cloud computing

4.3.1.3 Cloud computing services and deployment models

4.3.1.1 Awareness of records management and cloud computing

All participants from cloud computing service providers explained cloud computing as a solution or platform that allows for the management of electronic records online, records are stored on servers on or off premises and are accessed from different locations on various devices provided there is internet access. Respondent C1 highlighted that employees sit behind computers, tablets and other devices all day, creating documents, doing projects, or sending out quotes, which results in the production of invaluable data that needs to be protected and stored, hence the organisations' urge to adopt cloud computing. Respondent D1 highlighted that cloud computing for records management was simply having a contracted IT provider to store and manage the organisation's data without investing in IT infrastructure, such as hardware (servers), software and IT expertise.

4.3.1.2 Records management expertise for cloud computing

In researching cloud computing for records management, the study sought to examine the understanding of how issues of electronic records management were considered in the cloud. It emerged from the findings that two cloud computing service providers (Organisations B and C) did not consider equipping their staff with records management knowledge through records management training. In addition, Organisations B and C did not consider having a position for trained and skilled records management personnel. Organisation A indicated that respondent A3 was a records management staff who had acquired on-the-job training in records management.

The findings of the study also revealed that the organisations providing cloud computing services lacked records management expertise in their decisions to provide or outsource cloud computing solutions for records management. The study further established that cloud computing service providers used the word 'data' and 'information' (not records), for what they stored and managed on the cloud for their clients.

4.3.1.3 Cloud service(s) and deployment model(s) provided for records management

To analyse the cloud computing services and deployment models adopted for records management in Namibia, organisations were asked which cloud computing services and deployment models they provided for their clients. Table 4.2 below shows the results.

Table 4.2: Cloud services and deployment models provided by Namibian organisations

Organisations	Cloud services			Deployment models		
	IaaS	PaaS	SaaS	Private	Community	Public
Organisation A			✓	✓	✓	✓
Organisation B	✓			✓	✓	✓
Organisation C	✓	✓	✓	✓	✓	✓

Organisation A informed the study that they provided SAAS to their clients. Respondent A2 stated that, "We only provide the SAAS general solution".

Respondent B1 narrated that their cloud-hosting services included exchange (email), cloud backups, web hosting, IAAS and international domain registrations. Depending on client's requirements, the organisation offers Microsoft Azure, Microsoft Cloud and Office 365. These hosting services could be customised to clients' specifications. Organisation C indicated that they provided all services inclusive of IAAS, PAAS and SAAS. Respondent C1 respondent that their clients could choose the service(s) they wanted.

All organisations providing cloud computing (A, B and C) explained that they provided all deployment models - private, community and public - to their clients and the choice of deployment model(s) depended on the clients.

Respondent D1 was not sure which service or deployment model was adopted by their organisation. "That information is only known by the managing director", argued respondent D1.

4.3.1.4 Choosing a cloud service(s) and deployment model(s)

Participants stated that the choice of service and deployment model highly depended on client's requirements and affordability. Respondent C1 indicated that organisations were often worried about the location of their data when selecting a cloud-based solution. However, "what is actually important is who will have access to your data, and whether it will be available whenever needed", stated respondent C2. Respondent B1 further argued that that some clients opted to adopt two different deployment models - private and public - to cater to their different classes of data. They kept valuable or confidential data on a private cloud on the premises and the rest of their data on a public cloud at the vendor's data centre. Respondent A1 concurred by highlighting that clients preferred a hybrid solution where they kept some data on a private cloud and the rest on a public or community cloud on the providers' servers.

Due to the providers' contracts with their clients, no reference to clients were made. Additionally, no documents were shown due to confidentiality agreements between providers and their clients.

Respondent D1 mentioned that only top management was involved in the planning and implementation of cloud computing services in their organisation. The organisation developed a document explaining the processes and information that they manage, and the provider customised a solution for it. "I am not aware of the technical terms. We got a solution that worked for us," said respondent D1.

4.3.2 Assess if the factors which have driven the selected Namibian organisations to adopt cloud computing are related to records management

The second objective of the study sought to assess if the factors that had driven Namibian organisations to adopt cloud computing are related to records management. The findings to this objective are presented under the following sub-headings:

4.3.2.1 Cost of cloud computing for records management

4.3.2.2 Integration of legacy systems into cloud computing

4.3.2.3 Benefits of adopting cloud computing for records management

4.3.2.1 Cost of cloud computing for records management

The study intended to find out the cost of cloud computing services and how adopting cloud computing services can cut costs in organisations.

All participants highlighted that cloud computing might cut costs by providing organisations with IT infrastructure and expertise. Respondent B1 said that, "Organisations are provided cloud services in a cost-efficient manner via an internet connection on demand and on a subscription basis without having to invest in their own IT infrastructure that is costly". Respondent C1 responded that, "Cloud computing is affordable. However, it can be cheap or costly depending on how much storage space you need and the format of your data (videos, audios, music or documents)". Respondent A1 explained that cost depended on the number of licences needed by the client and the number of users. Respondent A3 added that outsourcing cloud services also cut hidden costs of printing, labour and storage. "There are also out of the box solutions that can be obtained for a minimal fee. However, "there is a need for customisation to accommodate each organisation's needs and specifications" stated A3. Respondent C1 indicated that there was no fixed cost for cloud computing services, as each client had different requirements.

4.3.2.2 Integration of legacy systems into cloud computing

Another aspect that the study sought to determine relating to drivers of cloud computing adoption was integration of existing business systems into cloud computing. Respondents were, therefore, asked to explain how the previous systems were integrated into the cloud computing solutions adopted. Cloud computing providers indicated that clients needed to decide on the existing data and systems needed to be integrated into the cloud solution they wanted to adopt. However, respondent C1 emphasised that integrating existing systems into the cloud was not without challenges. Respondent C2 stated that, “Some systems are outdated and inflexible, designed to perform one specific job which makes them cumbersome and sometimes costly to integrate”. Respondent A2 explained that the cloud services they provided allowed for the integration of existing systems such as emails and folder-based Windows solutions as well as other databases. “The email system of a client is directly linked to the cloud” asserted respondent A1.

Participant D1 from a cloud computing client was asked, “Which system(s) were used for records management before adopting cloud computing?” to which he responded, “Before cloud computing, a shared drive on the internal server was used to manage and access electronic records which could only be accessed on premises”. After the adoption of cloud computing, the records on the shared drive were migrated to the cloud solution. Respondent D1 informed the study that migrating data from a shared drive to the cloud solution adopted was a smooth process.

4.3.2.3 Benefits of adopting cloud computing for records management

The section presents data gathered on the drivers and benefits of adopting cloud computing for records management. Both cloud providers and client asserted that cloud computing offers irrefutable benefits to modern business operations. These benefits are presented in sections 4.3.2.3.1 to 4.3.2.3.3.

4.3.2.3.1 Improved staff productivity

Respondent A1 emphasised that with cloud computing, employees could fulfil their duties remotely, which could increase an organisation’s performance and productivity. Respondent D1 stated, “Everything is online, and you can access it from anywhere”.

Respondent A3 highlighted that "cloud computing eliminates the need to carry around a USB drive whenever you need to exchange or share information". The study established that one major benefit of cloud computing for records management was the ability to access records off premises, as it enabled employees to work remotely.

Respondent D1 narrated that, "Using cloud computing enabled us to switch from working on premises to working from home smoothly when the Covid-19 pandemic hit Namibia". The respondent further added that "business went on as usual, enabled by the cloud computing solution adopted". Using cloud computing enabled staff to work collaboratively on one document without having to send files back and forth between offices, which allowed for better document control, narrated respondent A3. The respondent went on to explain that since one version of the document could be worked on by different people, there was no need to have copies of the same document in circulation.

Respondents from organisation A highlighted that both public and private organisations were eager to explore cloud computing solutions due to the Covid-19 pandemic, which brought a drastic change in business operations. "Organisations are approaching cloud providers in search of flexible operating approaches to work during the pandemic which brought about a new normal," argued respondent A2.

4.3.2.3.2 Disaster recovery and business continuity

The study sought to establish the benefits of cloud computing relating to disaster recovery and business continuity. Respondent A3 narrated that cloud-based services provide quick data recovery for all kinds of emergency scenarios, from natural disasters to power outages. It eliminates the fear of losing valuable information due to malfunctioning or destruction of technology equipment. A1 added, "All the information uploaded to the cloud remains safe and easily accessible from any computer with an internet connection, even if the computer you regularly use stops working."

Respondent C1 argued that cloud computing enhanced business continuity through updated back up of data. Participants from cloud computing service providers (A, B and C) highlighted that whether clients experience a natural disaster, power failure or other crisis, their information stored in the cloud is backed up and protected in a secure and safe location. The ability to recover access to data quickly allows business to operate as usual, minimising any downtime and loss of productivity, explained respondent B1.

4.3.2.3.3 Competitive edge

Respondent A1 informed the study that cloud computing offered a distinct competitive advantage to its clients compared to organisations that are not using cloud computing. Respondent A2 added that cloud computing services offered clients the latest technology. In agreement, respondent B1 highlighted that their clients were ahead of their competitors by using cloud computing services, which helped them access the latest applications timely at low cost.

4.3.3 Assess the risks of managing records in the cloud experienced by the selected Namibian organisations

The third objective of the study sought to assess the risks of managing records in the cloud experienced by the organisations. Participants highlighted that there was no technology solution without risks. Cloud computing service providers emphasised that clients had to draw up their own requirements of how they wanted their data to be stored and managed. Organisations A, B and C highlighted that both the provider and client were responsible for the security of information in the cloud, depending on the service and deployment model adopted. Respondent B1 emphasised that it highly depended on the client who gets access to their data. Respondent A2 argued that, “Cloud providers put effort to configure security measures to protect clients’ information with the service they provide”. However, they cannot control how customers use the service, what information they add on it, and who has access to it. Respondent A1 explained that they had invested in high-quality technology to ensure their systems were safe from hacking and other cyber-attacks. Respondent C2 narrated that the providers’ security measures focused more on securing user access and end-to-end protection of the cloud environment. Respondent A2 highlighted that authentication rules were set for individual users and devices.

Respondent D1 indicated that they had some challenges with cloud computing in their organisation. The participant stated that it was challenging to access records when there was poor or no internet connection, resulting in the need to work on premises where good internet connection was assured.

Two key risks identified by the study findings addressing this objective are presented under the following sub-heading:

4.3.3.1. Legislative and regulatory security risks

4.3.3.2. Employees’ security responsibilities

4.3.3.1. Legislative and regulatory security risks

Respondents were asked to comment on issues concerning organisations’ legislative and regulatory requirements regarding electronic records management. Asked about the jurisdiction of the location where the records were stored and managed, respondent C1 stated that, “It feels better if you know for sure that your data is stored and backed-up in Namibia”. Respondent C2 added that an organisation could host its own data and be the master of its own data storage. All cloud computing service providers stated that they stored their clients’ data within Namibian borders. “Clients must understand their environment and inform us what they want, which will guide us to negotiate and agree on contracts", respondent B1 stated.

Respondents from organisation A indicated that the Namibian legal and regulatory framework, especially the Archives Act 12 of 1992, did not directly refer to the management of electronic records. This challenged and impacted the provision of cloud computing services to government institutions and both the cloud service providers and government institutions had to heavily depend on international standards to come up with standards and policies for managing records in the cloud. Participants did not show the researcher any SLA or any documentation due to confidentiality agreements between them and their clients.

The cloud computing client was asked whether their organisation had used any of the publicly available guidelines on cloud computing for records management. Respondent D1 did not know of any records management programme in place in their organisation or any guidelines that they referred to for implementing cloud computing.

4.3.3.2. Employees' security responsibilities

Cloud computing providers emphasised that cloud consumers needed to understand their role in cloud security to meet cloud security objectives of confidentiality, integrity, availability, authenticity, accountability, liability and privacy. Respondent B1 stated, "Cloud security is a shared responsibility." The client needed to take care of their devices and log-in credentials to avoid unauthorised access to their data. Respondent D1 reported that using cloud computing places a responsibility on all staff to always safeguard the organisation's information on all devices. It emerged in the study that it was a challenge to enforce the security of information on the cloud on different personal devices used by staff, such as cellphones and personal laptops. In addition, respondent D1 noted that there was fear of losing devices, such as cellphones, which posed a potential challenge of external access to organisation's information. "The organisation is putting faith on employees, as this is a challenging task to enforce," argued respondent D1.

4.3.4 Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations

The fourth and final objective of the study sought to identify measures employed by cloud computing service providers and clients to mitigate the risks of managing records in the cloud. Organisation C explained that to ensure the security of clients' data, they did not have access to the data of their clients. Respondent C1 stated, "We as the provider only have access to the backend of the cloud solution. This serves as "a guarantee that we cannot manipulate the integrity and authenticity of clients' data or know what information the client is keeping", posited respondent C2. On the other hand, respondent B1 highlighted that to ensure total security, clients were advised to adopt more than one deployment model, private for client's top valuable data and community or public for the rest of the data. However, this depended on affordability of servers and other necessary IT infrastructure and expertise. All participants stated that SLAs were in place, which both clients and providers agreed to and abided with. As already indicated earlier, no documentation was presented to the researcher upon request. Respondent A1 explained that their organisation used up-to-date firewalls to provide total security to clients' data and in addition they follow worldwide best practices concerning cloud security. Other approaches that were discovered by the study are discussed in sections 4.3.4.1 to 4.3.4.4.

4.3.4.1 Controlled Access

On the question: "How does the provider protect information and systems against unauthorised access?", the study found that there was controlled access by the clients.

The client decided who had access to which records explained Respondent A3. Respondent C1 explained that their organisation made sure that clients knew who had access to their data and what was done to their files via audit tracks and reports. The clients decided which users had what level of access to what data. Respondent C1 argued that it did not only give the organisation control, but it also streamlined the work, since staff knew documents assigned to them. Respondent A2 emphasised that every user, system or device required verification and validation before connection to the cloud solutions they provided to prevent unauthorised access to client's information.

Respondent D1 narrated that, "We have different access levels and permissions to documents, depending on [one's] position [in the organisation] to ensure each person in the organisation only has access to files regarding their work". Respondent D1 explained that these access levels were decided upon by the managing director and set up by the cloud services provider.

4.3.4.2 Cultivate Awareness

Awareness emerged as one of the mitigating factors of risks associated with cloud computing services. Cloud service providers highlighted that clients needed to create proactive security measures within their organisations, which encouraged a culture of security and compliance. Cloud service providers said they provided their employees with education and training related to cybersecurity awareness, which helped them spot advanced persistent threats, malicious insiders, system vulnerabilities, and other suspicious activities in cloud environments. Respondents C1 and C2 stated that providing security awareness training was part of the contracts with their clients.

Respondent D1 highlighted that general training was provided for the utilisation of the cloud solution to all employees by their cloud service provider. In addition, advanced training was conducted with selected staff members who were responsible to train other staff internally.

4.3.4.3 Security shared responsibility

Respondents were asked, “Who is responsible for records security in the cloud?” Respondent A1 argued that to achieve near perfect security, both provider and client needed to understand that cloud security was a shared responsibility and that they should work together to meet their security objectives. Respondent B1 posited that the security roles were outlined in the contracts they signed with their clients.

4.3.4.4 Audit trails

Asked how access was monitored in the cloud to minimise the risk of unauthorised access, cloud service providers indicated that audit trails, which informed the clients who did what, when and where to their data, were made available in the cloud. The study further probed how audit trails helped in mitigating cloud usage risks. Respondent B1 explained that audit trails timeously informed the clients of any malicious attempt to access, which prompted investigation and immediate action to strengthen security. Audit logs were accessed by the clients’ management team or whoever was given authority in the organisation. Respondent D1 explained that their top management had access to audit trail logs to ensure all staff only accessed what was assigned to them and to detect any external attempt to access data.

4.4 Summary

This chapter presented the data collected through interviews. The data from interviews was structured and analysed according to thematic areas. The researcher found three cloud computing providers who were willing to participate in the research and only one cloud computing client. Both providers and client understood cloud computing to be the solution for low-cost data storage and convenient flexible data access and usage.

The study established that organisations were aware of the benefits of cloud computing and advised that it was a solution more organisations needed to invest in due to its flexible working arrangements.

However, the data showed that there were risks in managing data in the cloud, specifically data security matters. Cloud providers made sure that they had strong cybersecurity to protect their client's data. The study established that the security of data in the cloud was the responsibility of both providers and clients of cloud computing solutions. Highlighting that there was no technology solution without risks and challenges, cloud service providers emphasised that there were measures they had in place to minimise them. Both the cloud provider and client have the responsibility to ensure that data are protected in the cloud. No documentations such as SLAs were shown to the researcher due to provider-client confidentiality agreements. The study also found that only top management from the cloud computing client organisation was involved in the decision of which cloud service, deployment model and provider to use. The study found that cloud-providing organisations lacked records management expertise on their workforce.

The next chapter discusses the findings.

CHPATER FIVE

DISCUSSION OF FINDINGS

5.1 Introduction

This chapter discusses and interprets the research data analysed and presented in Chapter 4. The aim of this chapter is to explore, discuss and explain the research data in relation to published literature on cloud computing for records management. Bui (2009) asserts that the discussion chapter is a vital component of a study because it is where research data is interpreted in a meaningful way and the implications are made clear to the reader. In agreement, Hess (2004) opines that research findings discussion gives the reader a meaningful view of the study. This study's purpose was to assess the use of cloud computing for records management in Namibia. This chapter is structured according to the following objectives and themes that emerged from content analysis as presented in Chapter 4:

- ▪ Analyse the cloud computing services and deployment models adopted by the selected Namibian organisations:
- Awareness of records management and cloud computing
- Records management expertise for cloud computing
- Choosing cloud services and deployment models for records management
- ▪ Assess if the factors which have driven the selected Namibian organisations to adopt cloud computing are related to records management:
- Cost of cloud computing for records management
- Integration of legacy systems into cloud computing
- Benefits of adopting cloud computing for records management:
- Improved staff productivity
- Disaster recovery and business continuity

- Competitive edge
- Assess the risks of managing records in the cloud experienced by the selected Namibian organisation:
- Legislative and regulatory security risks
- Employees’ security responsibilities
- Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations:
- Controlled access
- Cultivate awareness
- Security shared responsibility
- Audit trails

5.2 Analyse the cloud computing services and deployment models adopted by selected Namibian organisations

5.2.1 Awareness of records management and cloud computing

The study established that cloud computing service providers see cloud computing as a solution or platform that allows for data management online and data storage on servers on or off premises and the access of data from different locations on various devices where there is internet access. It was evident that the selected Namibian organisations providing and using cloud computing were aware of the overall meaning and operations of cloud computing. However, the aspect of records management was absent. This can have tangible impacts on records management and compliance. This finding is similar to King (2019), who argues that if the cloud solution adopted does not successfully tackle all three elements, that is, records management, data management, and information governance, it will lead to complications.

When asked about the drive for using cloud computing for records management, cloud computing providers highlighted that there was a realisation that employees created a huge volume of data daily that needed to be stored and accessed effortlessly. This finding is similar to that of Farrell (2010) who reports that organisations are faced with constant technological change, ageing infrastructure and software, shrinking budgets, and a global and mobile workforce. The study established that in the selected Namibian organisations, the word ‘data’ was loosely used by cloud service providers to refer to records. Rice (2022) opines that records contain data, however, the records themselves are not data. Consequently, data management is concerned with ensuring the data within those records can be used by the organisation. A study done by Kibe (2016) discovered that there is a rise in the adoption of cloud-based services, with most organisations seeking efficient and cost-effective technology solutions while others are hoping to cut costs, eradicate redundancies and pool resources with low consideration of electronic records management functional requirements.

5.2.2 Records management expertise for cloud computing

In researching cloud computing for records management, the study sought to examine the records management expertise applied to the development and adoption of cloud computing services for managing records. It is normally clearly mentioned on ICT service providers’ websites that they provide electronic records management solutions. However, information management systems are typically developed by IT technicians for reasons other than to keep records, most often to automate business activities or processes, while record-keeping systems are required to serve a more specific purpose, such as capture and preserve evidence of business transactions, whether for administrative, legal, or historical value. This is a challenge mentioned by a records manager in Schneider (2021)’s survey that it is difficult to bring records management to systems built around datasets rather than documents. The records manager further claims that records that are supposed to be collected in forms is now being inserted into databases and reconfigured for reporting, trending and approval (Schneider, 2021). Serious thoughts need to further be applied to the expertise applied in designing the solutions and the problems they are designed to solve.

Bernbom, Lippincott and Eaton (1999) advise that information technologists should be aware that the information systems they are responsible for developing may be serving a broader purpose than automating business processes during their original design. Archivists and records managers can be valuable allies to information technologists in helping to ensure that these systems are reliable and useful for the many purposes they will be expected to serve.

Bernbom et al. (1999) strongly argue that archivists and records managers have historically had the responsibility of ensuring organisations' long-term access to records, however, many new challenges of lack of certainty regarding basic records management functionality in commercial cloud solutions for managing electronic records are apparent in the networked environment. A study by Runardotter (2007) found that there was a lack of knowledge in records and archives management mainly among management and IT personnel, yet they set and develop digital information management standards, design and implement systems and develop ICT policies with no involvement of records management personnel.

5.2.3 Choosing cloud computing services and deployment models for records management

Cloud computing service providers noted that cloud services and deployment models highly depend on clients' needs and their demands derived from their business types and operations. This study did not establish the reason behind the type of service(s) or model(s) provided by the selected Namibian organisations. However, it was revealed that clients were required to specify the service and deployment model they preferred. The study was further informed that organisation C provided all types of services, including of IaaS, PaaS and SaaS. While organisation A provided only SaaS to their clients. Organisation B provided IaaS, which can be customised to clients' specifications. Technology solutions mostly are not designed to address all information management aspects, and in most cases, organisations are not able to afford different solutions for each aspect – data management, document management, workflow, and records management with long-term preservation (McLeod & Gormly, 2017). This finding is similar to Rice (2022) who argued that organisations needed to have separate solutions to manage different information functions, which is highly unaffordable.

The study was informed that the choice of deployment model(s) highly depended on a client's requirements and affordability, making the decision to move to the cloud a complex task and it highly depends on an organisational context. This resonates with the argument by Diaby and Rad (2017) that a successful cloud computing implementation depends on choosing the right deployment model for each organisation or category of information. This argument is in support of Rountree & Castrillo, (2013) who posit that different organisations will be satisfied by different deployment models depending on their organisational needs, operations and budget.

Cloud computing providers further informed the study that they provided all deployment models - private, community and public to their clients - and the choice of which deployment model(s) to use depended on the clients. However, most organisations opted to adopt two different deployment models - private and public - to cater for their different classes of data. They kept data regarded as valuable or confidential on a private cloud on the premises and the rest of their data on a public cloud at the vendor's data Centre. This is mostly done according to the need for customisation and security concerns. The findings of this study are similar to those of Robinson (2010) argues that organisations can store some data on a public cloud and leave the more sensitive information on a private cloud. This is of particular benefit to records management as the most valued records can get the much-needed security offered by private cloud.

5.3 Assess if the factors which have driven selected Namibian organisations to adopt cloud computing are related to records management

5.3.1 Cost of cloud computing for records management

The study intended to find out the cost of cloud computing services and how adopting cloud computing services can cut cost for organisations efforts to effectively manage electronic records. The study participants highlighted that cloud computing certainly cut cost by providing organisations with IT infrastructure and expertise.

Cost-efficiency is the highest occurrence on Carroll et al. (2011)'s graph of cloud computing benefits. This implies that most cloud computing users are reaping the cost-cutting benefit of using of cloud computing as it provides great savings in IT-related costs, such as expertise, hardware and software. The results of this study agree with Carroll et al. (2011)'s findings that organisations are provided cloud services in a cost-efficient manner via an internet connection on demand and on a subscription basis without having to invest in their own IT infrastructure that is highly costly. Prasath et al. (2013) concur with the findings that cloud computing services are outsourced through a pay-per-use system, which implies that just like electricity or municipality water, IT services are charged per usage metrics – pay per use. The more you use, the higher the bill and vice-versa.

Despite cloud computing services praise over cutting costs, Farrell (2010) argues that the key to the selection and usage of cloud technologies and related services by a client organisation is an understanding of the top enterprise security priorities. This entails improving information security risk management, implementing/improving data loss prevention technologies and processes, security awareness and training, regulatory compliance, security testing, and implementing/improving identity and access management technologies and processes that are very costly. The study established from cloud computing providers that cloud computing can be cheap or costly depending on the service(s) and deployment model(s) adopted and on how much storage space an organisation needs and the format of the data (videos, audios, music or documents). The cloud computing providers explained that cost also depended on the number of licences needed by the client and the number of users.

Rosencrance (2020) argues that cloud computing can offer organisations potential financial advantages, however, it is important to understand the full implications of cloud pricing, and how it can affect the organisations' information management. Cutting costs should not result in a lack of due diligence when selecting cloud services and deployment models for organisations adopting cloud computing for records management. For example, it is cheaper to adopt a public or community cloud deployment model, however, it becomes expensive as it has limited information security (information loss, leakage or cyber-attacks), and reliability issues (time loss in accessing records). The above argument is supported by Hidalgo (2013), who highlights that additional costs for integration, end-user support, upgrade management, security, compliance, testing and workflow may be incurred for effective records management in the cloud.

5.3.2 Integration of legacy systems into cloud computing

According to Hainaut et al. (2008), legacy systems are software solutions made up of large and ageing programmes relying on legacy database systems found and used by an organisation for a long period of time. Responding to the question: "how are the previous systems integrated into the cloud computing solutions adopted?", cloud computing providers indicated that clients needed to decide which existing systems needed to be integrated into the cloud solution they want to adopt. This aspect was explored in order to understand workflow and integration of existing electronic records into cloud services.

The cloud providers stressed that integrating existing systems into the cloud was not without challenges as some systems were outdated and inflexible, designed to perform one specific job, which makes them cumbersome and costly to integrate. This finding is similar to those of Zalazar, Gonnet and Leone (2015), whose studies found that legacy information systems usually work in isolation and have exclusive data repository, which make the communication between the legacy systems to other newer application a complex task, as it requires the definition of complex communication interfaces and data conversion components. Additionally, Leone (2015) claims that organisations with old legacy systems need to invest money to integrate their tools and adapt functionality to new technologies.

This study found that the cloud services provided by cloud providers allowed for the integration of existing systems such as emails and folder-based Windows solutions, as well as other databases, despite challenges of integration. This supports Fahmideh et al. (2017), who argue that migration is an expensive and complex process, however, it greatly increases the information system control and evolution to meet future business requirements.

5.3.3 Benefits of adopting cloud computing for records management

Various scholars (Kibe, 2016; Mosweu et al., 2019; Marutha & Ngulube, 2012; Bassett, 2015; Chitauro, 2017; Carroll et al., 2011) have observed that cloud computing has a potential of offering good electronic records management solutions and benefits to records managers, as it facilitates fast delivery of information and provides huge space for the storage of records. Additional advantages associated with cloud computing for records management include cost-saving, enhanced accessibility, better centralisation, increased flexibility, having access to records even in times of disaster, and improved interaction with the user community (Kibe, 2016; Mosweu et al., 2019).

This study sought to find out the reasons that led organisations to adopt cloud computing for records management and how those reasons were addressed. The study established that both cloud providers and client were aware of the benefits offered by cloud computing and its importance to modern business operations. These benefits are discussed in sections 5.3.3.1 to 5.3.3.3.

5.3.3.1 Improved staff productivity

Improved staff productivity was one of the top cloud computing adoption benefits mentioned by the study's participants. Organisation A emphasised that with cloud computing, employees can fulfil their duties remotely, which increased an organisation's performance and productivity. This finding is in agreement with Kibe (2016), who argues that cloud-based services have a huge capacity to facilitate remote access to records, online collaboration and file sharing with multiple users, thus enhancing an organisation's staff productivity and output. The findings of this study revealed that cloud computing is offering good records management solutions to organisations, as it facilitates fast delivery of information. This finding corroborates the finding of the study done by Kibe (2016), which established that cloud-based services enhanced records retrieval time, therefore, it accelerated the decision-making process in Kenyan public institutions. Kibe found this a critical benefit, as timely availability of records was a challenge most public institutions in Kenya faced, which resulted in delayed service delivery. Matangira (2016) found that the main source of recordkeeping challenges in the public service of Zimbabwe was due to the lack of ICT incorporation into their records management and service delivery operations.

Cloud computing providing organisations highlighted the rapid increase of cloud computing adoption amid the Covid-19 pandemic. Iron Mountain Incorporated (2020) conducted a survey on the impact of Covid-19 on RIM, which established that most organisations had to change the way they operated, and this impacted their records and information management programmes. The survey found that most organisations had digitised records and automated workflows to make provision for remote work. This study established that one major benefit of cloud computing for records management was the ability to access records off premises, which enabled employees to work remotely during the pandemic. The cloud computing client narrated that using cloud computing enabled the organisation to switch from working on premises to working from home smoothly when the Covid-19 pandemic hit Namibia. In agreement, cloud computing providers indicated that the pandemic had opened many organisations eyes both public and private to the ability, potential and need of cloud computing services resulting in many organisations approaching cloud computing providers in search of flexible operating approaches to work during the pandemic, which brought about a new normal. Ncaagae-Mbe (2021) highlights the major impact Covid-19 lockdowns had on records management that the Botswana Communications Regulatory Authority moved its services online to enable access to information.

Staff productivity is enhanced by cloud computing, as it facilitates the realisation of multi-user access to records thereby enabling ready access to records and real-time collaboration in decision making and task performance in organisations. Mosweu et al. (2019) confirm the flexibility of access to records managed in the cloud in their study that claims that records in the cloud are accessible to user remotely over the internet, enabling staff to be more flexible to access, work and share documents while away from the office via multiple devices.

5.3.3.2 Disaster recovery and business continuity

Records management is an important recovery aspect to dealing with a disaster as it is where an organisations' memory resides (Long, 2020). Recovery can be difficult for an organisation after losing records to a disaster. Business continuity is defined by the National Archives of Australia (2018) as planned activities undertaken by an organisation to ensure that critical business information remains available despite a disaster or disruption. It stretches from simple decisions like backups and disaster recovery software, to the steps taken to get a business back to normal. The study findings indicated that cloud computing provided quick data recovery for all kinds of emergency scenarios, from natural disasters to power outages which eliminated the fear of losing valuable information due to malfunctioning or destruction of technology equipment. Cloud providers claimed that all the information uploaded to the cloud remained safe and easily accessible from any computer with an internet connection, even if the computer one regularly uses stopped working. The above finding is similar to that of Long (2020), who argues that records management systems need to be designed to capture documents and data, replicating them to disaster-safe storage to avoid significant data losses in the event of major outages.

The study found that cloud computing enhanced business continuity through updated back-up of data. Cloud computing service providers highlighted that whether clients experience a natural disaster, power failure or other crisis, their information stored in the cloud was backed up and recoverable. The ability to regain access to data quickly allows business to operate as usual, minimising any downtime and loss of productivity. The business continuity and disaster recovery capabilities of cloud computing are positive examples of the viability of cloud services for data storage and records management, particularly regarding the automatic replication of data. This finding is similar to that of the Cloud Security Alliance (2012) that business continuity and disaster recovery are requirements when using cloud services. This assures clients that their records are backed up and/or replicated to be available in case disaster strikes.

Beagrie, Charlesworth and Miller (2014) highlight that cloud services can provide automatic data replication to multiple locations and access to professionally managed digital storage. In addition, cloud services provide access to other dedicated tools, procedures, workflow and service agreements, tailored for digital preservation requirements. Cloud computing may be a good solution for digital preservation of records when cloud providers put in place mechanisms to migrate digital records as hardware and software migrates to newer versions. In addition, the Open Archival Information System (OAIS) model defines a broad range of functions including ingest, access, archival storage, data management and administration, including digital preservation (Askhoj, Sugimoto & Nagamori, 2011). Digital preservation functions other than archival storage can be provided via the cloud. However, the findings of this study established that cloud providers are more focused on providing storage and IT expertise for their cloud clients.

5.3.3.3 Competitive edge

The competitive business environment requires organisations to respond quickly to business demands. As a result, cloud computing serves is an enhanced technology that has become vital in running a business. Cloud computing providers informed the study that cloud computing services offered clients the latest technology applications timely and cost-effectively. These offered them a competitive advantage compared to organisations not using cloud computing services. This finding is similar to that of Thomas (2009), who acknowledges that cloud computing acts as an excellent technological tool as it offers a wide range of solutions and advantages to business that permit the users and consumers to integrate and combine a variety of services to increase creativity and productivity. Similarly, Mosweu et al. (2019) argue that the world business community has become competitive to such an extent that an organisation cannot survive using the traditional ways when conducting business.

5.4 Assess the risks of managing records in the cloud experienced by the selected Namibian organisations

Convery (2010b) outlines that outsourcing of information storage and services to the cloud creates various risks, particularly risks concerned with information security, compliance, loss of information and unauthorised access (Convery, 2010b; Carroll et al. 2011; Yimam & Fernandez, 2016; Ngoepe & Saurombe, 2016). Organisations that participated in this study were aware that there was no technology solution without risks. Cloud computing service providers emphasised that clients needed to draw up their own requirements of how they want their data to be stored and managed. It was further established that both the provider and client shared the responsibilities of ensuring security of information in the cloud, depending on the service and deployment model adopted.

InterPARES (2018) reveals that cloud computing has not yet been made part of electronic records management in most African countries. The reuse of information and subsequent changing of context of information created online is often beyond the control of an organisation. The most obvious records management question is how a records manager maintains and manages a record when it is constantly changing beyond the parameters of the organisation. Some records professionals may even argue that if web records do not satisfy the archival diplomatic elements (medium, content, physical form, intellectual form, action, persons, archival bond and context) then the information is not a record at all (Stuart & Bromage 2010). Government of South Australia (2015) guidelines further define the record-keeping challenges associated with cloud computing, including "a loss of access to records", "record destruction or loss", and the risk that the "evidential value of records may be damaged".

The cloud computing client responded that it was challenging to access records when there was poor or no internet connection, necessitating the need to work on premises where there is good internet connection. This finding is similar to that of Wamuyu (2017), who argues that the digital divide was one of the greatest challenges for developing countries when it came to the use of ICTs due to poor access to internet. Cloud computing services are strictly web-based, and lack of internet access adversely affects their adoption and organisations cannot completely reap their benefits such as remote access.

The two major risks identified by this study are discussed more in sections 5.4.1 and 5.4.2.

5.4.1 Non-compliance to legal and regulatory framework

The management of records in the cloud is subject to legal and regulatory requirements. However, in practice, cloud vendors do not often specify where a client organisation's information is physically stored, including their distributed server environment, which can result in client data being stored in more than one jurisdiction (Kabata, 2012). The study was informed that clients preferred to know where their information was stored, and they were comfortable with having their information stored and backed-up in Namibia. Cloud computing providers informed the study that organisations had the option to host their own data and be masters of the storage. All cloud computing service providers stated that they stored their clients' data within Namibian borders. Duranti and Jansen (2013) highlight that storing information in a separate jurisdiction has legal and liability risks.

Participants were asked on issues concerning the organisations' legislative and regulatory requirements regarding electronic records management. The study established that participants were unaware of the regulatory framework for the management of digital records in Namibia. It further emerged in this research that the government has not publicised specific legislation for managing electronic records. The Archives Act 12 of 1992 did not directly refer to the management of electronic records or use of ICT in the management of records. The Act was promulgated with paper records in mind. The study established that the lack of direct legal and regulatory framework for electronic records management challenged and impacted the provision of cloud computing for government institutions and these institutions have to heavily depend on international standards to come up with standards and policies for managing records in the cloud.

Other studies done in African countries have made similar observations of weak legislation for electronic records management. Non-compliance with legal requirements is a challenge in African countries due to inadequate and outdated legislation relating to records archives management, as found by different scholars

(Asogwa, 2012; Mosweu, 2012; Ngoepe & Saurombe, 2016). In the Namibian context, these observations were supported by scholars (Nengomasha, 2009; Barata et al., 2001) whose studies found that there was an absence or weak legislative and policy frameworks for electronic records management. However, Namibia has enacted an Electronic Transaction Act 4 of 2019 that aims to develop, promote and facilitate electronic transactions and related electronic communications (Office of the Prime Minister, 2019). Despite the enactment of this Act, the study found that participants were not aware of it and its application to cloud computing. This may be due to the lack of records management expertise discussed in section 5.4. The Electronic Transactions Act does not give guidelines for adopting systems and technology solutions for electronic records management.

Literature indicates that policies have a huge impact on how records are stored in any country (Ngoepe & Saurombe, 2016). The participants informed the study that the compliance aspect of cloud computing is a shared responsibility for both the client and the provider. This finding is similar to that of Yimam and Fernandez (2016), who opine that in cloud computing, compliance is a shared responsibility for client organisations, providers, service brokers and auditors. As fundamental aspects of law, records evaluation should be considered not only for accessibility and business purposes but also for accountability, reliability and evidential requirements. Ngoepe and Saurombe (2016) suggest that to enable proper management and preservation of digital records, there is a need for an archival legislation that embraces records created and stored in the networked environment.

5.4.2 Employees’ security responsibilities

Cloud computing providers emphasised that it is the cloud consumer’s responsibility to understand their role concerning the security of information in the cloud and to meet cloud security objectives of confidentiality, integrity, availability, authenticity, accountability, liability and privacy. The study was further informed that cloud security is a shared responsibility by all stakeholders. The client needs to understand their security responsibilities and take care of their devices and log-in credentials to avoid unauthorised access to their data. Sen (2015) posits that the rise in smartphone usage may expose information stored in the cloud due to lack of rich application programming interfaces (APIs) that support network communications and background services. The study found that as much as cloud providers need to secure their services, clients needed to understand that the use of such services places a responsibility on all staff to safeguard the organisation's information at all times on all devices. It emerged in the study that it was a challenge to enforce the security of information in the cloud on different personal devices used by staff such as cellphones and personal laptops. In addition, the study noted that the client organisation feared staff losing devices such as cellphones, which posed a potential challenge of external unauthorised access to organisational information. The study was informed that the only remedy to this challenge was for the organisation to have faith in its employees, as this is a challenging task to enforce. These findings are similar to those of McDade (2022), who argues that employees may become insider threats due to negligence or lack of adequate training and common human errors stemming from losing personal devices with cloud accounts to using weak passwords for cloud accounts.

5.5 Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations

One of the study objectives was to identify measures employed by cloud computing service providers and clients to mitigate the risks of managing records in the cloud. The findings revealed that cloud computing providers ensured the security of clients' data by avoiding having direct access to the data of their clients, but rather have access to the back-end of the cloud solution only. This served as an assurance that clients' information's integrity and authenticity could not be manipulated. Goldin (2017) disagrees, arguing that to provide a cloud service the provider must have access to the data stored, however, access can be limited to certain personnel on the provider's taskforce. Sen (2015) proposes two approaches for maintaining confidentiality of data in the cloud and limiting privileged user access: first, encryption of the data prior to entry into the cloud and, second, legally enforcing the requirements of the cloud provider through contractual obligations and assurance mechanisms to ensure that confidentiality of the data is maintained based on required standards.

The study was further informed that cloud providers advised clients to adopt more than one deployment model, private for client's top valuable data and community or public for the rest of the data in order to enhance security. However, this depended on the affordability of servers and other necessary IT infrastructure and expertise by clients. The study found that it is the providers' responsibility to employ up-to-date firewalls to provide total security to clients' data and also follow worldwide best practices concerning cloud security. The study was informed that SLAs were in place which both clients and providers agreed to and abided with. The Government of South Australia (2015) advises organisations to establish contractual arrangements to manage cloud computing known risks and to monitor those arrangements. Organisations are also urged to do due diligence and a thorough risk assessment before entering arrangements or contracts with cloud service providers.

Other approaches that were discovered by the study are discussed in sections 5.5.1 to 5.5.4.

5.5.1 Controlled access

Responding to the question interview question: “How does the provider ensured the information and systems were protected against unauthorised access?” the study found that there was controlled access by the providers. It was the client who decided who gets access to which records. Strong authentication is a mandatory requirement for any cloud solution. User authentication is the basis for access control in the cloud environment. Authentication and access control are more important than ever since the cloud and all its data are accessible to anyone over the internet (Sen, 2015). It was explained in this study that cloud service providers ensured that their clients outlined who had access to their data and what was done to their files via audit tracks and reports. It is, however, the client’s responsibility to outline their access levels for information stored in the cloud based on the staff. The clients decided which users had what level of access to what data. The study was further informed that every user, system or device required verification and validation before connection to the cloud solutions they provided to prevent unauthorised access to clients’ information.

The cloud computing client organisation informed the researcher that they had different access levels and permissions to documents, depending on job positions to ensure each person in the organisation only has access to files regarding their work. These access levels were decided upon by the managing director and set up by the cloud services provider.

It is the cloud services provider’s responsibility to configure security measures to protect the client’s information with the service they provide, however, they cannot control how customers use the service, what information they add on it, and who has access to it. The study found that providers had invested in high quality technology to ensure their systems were safe from hacking and other cyber-attacks. The providers’ security measures focused more on securing user access and end-to-end protection of the cloud environment. Convery (2010a) argues that it is the cloud providers' responsibility to demonstrate existence of effective and robust security controls, assuring customers that data and applications are adequately secured against unauthorised access, change or destruction.

5.5.2 Cultivate awareness

Awareness emerged as one of the mitigating factors of risks associated with cloud computing services from the study. Cloud service providers highlighted the need for clients to create proactive security cultures within their organisations that boost security and compliance. Romeo (2020) opines that human error is a strong attack vector for many popular cybercrimes, and the best way of enhancing any security programme is to create a cyber-aware workforce. Cloud service providers informed the study that they educated their employees and offered them training related to cybersecurity awareness, which helped them spot advanced persistent threats, malicious insiders, system vulnerabilities, and other suspicious activities in cloud environments. The study found that providing security awareness training was part of the contracts with their clients.

In confirmation, the cloud computing client organisation informed the study that general training was provided for the utilisation of the cloud solution to all employees by their cloud service provider. In addition, advanced training was conducted with selected staff who were responsible to train other staff internally. Developing and implementing a cybersecurity policy can be a good way of clearly communicating to employees what is expected of them when it comes to the organisation's security practices (Romeo, 2020). This is particularly relevant to a situation reported in section

5.4.2, where the organisation relies on trust that employees will do the right thing regarding the security of their devices.

5.5.3 Security shared responsibility

Security shared responsibility was raised as a security mitigating factor by the respondents. Cloud Security Alliance (2020) claims that understanding where a cloud provider's responsibility ends, and where a clients' security responsibility begins is a key factor to a successful security implementation in a cloud environment. To achieve near-perfect security, both provider and client need to understand that cloud security is a shared responsibility and that they should work together to meet their security objectives. It is a requirement that cloud providers and clients share the responsibility for security and privacy in cloud computing environments (Takabi, Joshi & Ahn, 2010). The study was further informed that the security roles for both the client and provider were outlined in SLA. The extent to which the provider is responsible for security is also determined by the type of cloud service and model. For example, SaaS providers are more responsible for security and privacy in comparison to PaaS and IaaS providers (Takabi et al., 2010). The cloud security responsibility varies by deployment model. For example, in a private cloud, the client is responsible for the security of the entire operating environment, inclusive of applications, physical servers, and user controls; compared to a public or community cloud where security responsibilities are widely shared by both the client and provider (Center for Internet Security, 2021).

5.5.4 Audit trails

Audit trails maintain a record of the system's activity both by the system and application processes and by user activity on systems and applications (NSIT, 2011). Cloud service providers indicated that audit trails, which informed the clients who did what, when and where to their data, were made available in the cloud to trace unauthorised access. The study further probed how audit trails aided in mitigating cloud usage risks. Audit trails timely informed the clients of any malicious attempt to access the records, prompting investigation and immediate action to strengthen security. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications (Marker, 2022). Audit logs were accessed by the clients' management team or whoever was given authority to do so in the organisation.

5.6 Summary

The chapter discussed the study findings and how they compare with related studies on cloud computing and records management.

The findings revealed that Namibian organisations are using cloud computing for data storage. The consideration of electronic records management legislations and standards was found to be lacking. Organisations providing cloud computing lacked records management expertise. This may threaten the authenticity, reliability, integrity and usability of the data stored on the cloud. Despite the risks and challenges of managing records in the cloud, the study established that there were benefits of using cloud computing in this modern world. Cloud service providers emphasised that there were measures in place to mitigate identified security risks of cloud computing. Both the cloud provider and client had a responsibility to ensure that data was protected in the cloud.

Between the benefits and risks of using cloud computing, it came out clearly that the type of cloud service and the deployment models play a significant role in determining the successful implementation and usage of cloud solutions for records management. However, the study established that participants did not display knowledge of which cloud service model is viable for records management. It came out clearly that cloud computing was mostly adopted for storage, workflow and cost-cutting. The study further established that Namibia's poor electronic records management legal framework has a significant impact on the adoption of cloud computing solutions.

The next chapter provides a summary of the findings, the conclusions and recommendations.

CHAPTER SIX

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

In this final chapter, the study findings are summarised, the research is concluded, and recommendations are proposed. The aim of the summary is to provide an overview of the study and to indicate the line and progression of reasoning of this research (Jacobs, 2014). The chapter is divided into three sections: the summary arranged according to the study objectives, the conclusion arranged according to the study objectives, and the recommendations that include a cloud computing deployment model for records management in Namibia.

6.2 Summary of Findings

The study's findings are summarised according to the study objectives below:

- Analyse the cloud computing services and deployment models adopted by the selected Namibian organisations
- Assess if the factors which have driven the selected Namibian organisations to adopt cloud computing are related to records management
- Assess the risks of managing records in the cloud experienced by the selected Namibian organisation
- Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations.

6.2.1 Analyse the cloud services and deployment models adopted by the selected Namibian organisations

Evident from the study is that selected Namibian organisations were providing and using cloud computing for data storage and management. However, there is apparent lack of awareness of records management and electronic records management functional requirements. The word data was used to refer to records by cloud computing providers. The use of these terms loosely can have a negative impact on records management. It is, therefore, crucial to note that the selected organisations providing cloud computing services lacked records management expertise in their decisions to provide or outsource cloud computing solutions for records management. The absence of records and archives management qualified personnel in organisations providing cloud computing services resulted in a lack of records management expertise in the designing and adoption of cloud services. It further resulted in the use of the word data to refer to information stored and managed in the cloud. Cloud service providers lacked the understanding of records management despite their claim of the solutions' ability to manage records. Records and archives management staff were further not involved in the adoption of cloud services from the client organisation.

A client's needs, business operations and budget determine the cloud service type and deployment model. Cloud computing providing organisations provided one or more service type (IaaS, PaaS, and SaaS) and deployment models (private, public, community and hybrid). Some organisations adopted two deployment models to cater for different classes of data for security purposes.

6.2.2 Assess if the factors which have driven selected Namibian organisations to adopt cloud computing are related to records management

The cost of cloud computing highly depends on the service type and deployment model adopted – it can be cheap or expensive. The study further found that storage, media format and number of licences had an impact on the cost of cloud computing.

Cloud computing adopted by Namibian organisations allowed the integration of legacy systems based on clients' requests and the ability of the solution. Integration was found to be challenging for outdated and inflexible systems. This study found that the cloud services provided by cloud providers allowed for the integration of existing systems such as emails and folder-based Windows solutions as well as other databases, despite challenges of integration.

Both cloud computing providers and the client organisation realised that cloud computing offers various benefits to business operations. Improved staff productivity came out as a major benefit in recent years due to the Covid-19 pandemic. The use of cloud services allowed employees to work remotely provided they had internet connection. Cloud computing further allowed employees multi-user access to documents and work and share features. It further emerged from the study that cloud computing solutions provided back-up data storage for disaster recovery and business continuity purposes. The ability to recover access to data quickly allows business to operate as usual, minimising any downtime and loss of productivity. It is argued by cloud providers that adopting cloud computing services offers clients a competitive edge by making available latest technology applications to maximise productivity.

6.2.3 Assess risks of managing records in the cloud experienced by the selected Namibian organisations

The study found two major risks of managing records in the cloud in the selected Namibian organisations - non-compliance to legal and regulatory laws pertinent to records management and poor security. These risks were a result of a poor legislative and regulatory framework for electronic records management, and employees' security responsibilities.

Namibian legislations on records management, such as the Archives Act 12 of 1992, do not directly refer to the management of electronic records or usage of ICTs systems in the management and use of records. Namibia enacted the Electronic Transaction Act 4 of 2019, which aims to develop, promote and facilitate electronic transactions and related electronic communications. However, it does not clearly show how records emanating from those transactions should be managed. Despite this, due to the lack of records management expertise in organisations adopting and providing cloud computing, participants were unaware of legislative and regulatory requirements regarding electronic records management.

The security responsibility placed on cloud computing clients was found to be a risk, as clients needed to ensure their devices are not accessed by external people by protecting their log-in credentials. Organisations placed trust and faith in their staff to enforce the above. It was evident that organisations were challenged with enforcing this due to the usage of staff personal devices such as mobile phones and laptops that can easily be stolen and hacked.

6.2.4 Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations

The study aimed at identifying measures employed by cloud computing service providers and clients to mitigate the risks of managing records in the cloud. Adopting more than one deployment model mitigated the risk of poor security for sensitive data by storing it on a private cloud and storing other business information on a public or community cloud. This approach has cost implications. The study learnt that it was the providers' responsibility to invest in up-to-date firewalls to provide total security to clients' data and, in addition, to follow worldwide best practices concerning cloud security.

User authentication and access levels were used to prevent unauthorised access to cloud solutions. Access levels were allocated by the clients according to staff portfolios. Despite the cloud provider's responsibility to configure security measure, it is the client's responsibility to control internal access – shared security responsibility. Audit trails were also put in place to track the solutions usage timely. Audit logs were accessed by the clients' management team or whoever was given authority in the organisation. Cybersecurity awareness training was conducted with clients to cultivate a culture of awareness as a security mitigating factor.

6.3 Conclusions

This section presents the conclusions from the study and is arranged according to the study's objectives.

6.3.1 Analyse the cloud computing services and deployment models adopted by the selected Namibian organisations

The selected Namibian organisations provided all cloud service types and deployment models. However, it was not evident whether the decision to adopt these services and deployment models was based on electronic records management functional requirements, records security or cost.

Moreover, despite records management being highly affected by the rapid development of ICTs, the study established that cloud computing service providers did not employ professional records and archives management personnel, nor did they equip their staff with the knowledge of records management through records management training. Thus, the poor understanding of records management resulted in the use of the word 'data' to refer to information stored, managed and used in the cloud, as stated in section 5.2. It has come out clearly in this study that records management staff were not involved in the adoption of cloud computing from both the cloud computing providing organisations and cloud computing client organisation.

6.3.2 Assess if the factors which have driven the selected Namibian organisations to adopt cloud computing are related to records management

It is evident from the findings that cloud computing offers benefits to the management of information by enhancing productivity, allowing remote information access and ICTs infrastructure cost. One aspect that directly stands out in this study is the ability to access information stored on the cloud anywhere over different devices over the internet.

6.3.3 Assess the risks of managing records in the cloud experienced by the selected Namibian organisations

The study established the following as risks: weak legal and regulatory framework for electronic records management in Namibia; non-compliance with Namibia’s laws for managing records; a lack of awareness by cloud service providers of national and international standards and requirements for electronic records management; a lack of skilled and experienced staff; poor internet connectivity and security.

6.3.4 Identify measures employed to mitigate risks of managing records in the cloud by the selected Namibian organisations

The study identified controlled access via user authentication and access levels as the top security mitigating factor for the client organisations. Security awareness trainings and audit trails were used to provide evidence of usage and access to information stored in the cloud.

6.4 Recommendations

It is evident that the selected Namibian organisations are using cloud computing to store and manage records, however, with little knowledge of electronic records management functional requirements, legal and regulatory framework considerations and expertise of records management. The study, therefore, recommends the following:

6.4.1 Compliance

The study recommends the revision of both the Archives Act and the Archives Code and the development of policies to address e-records and e-governance, digital preservation, electronic records management functional requirements and disaster recovery. This should be done through open dialogue and consultations between records and archives management, and information and communication technology professionals.

Organisations adopting cloud computing to manage records should familiarise and comply with the Electronic Transaction Act 4 of 2019 to raise above risks associated with cloud computing such as loss of records due to contract terminations, and records manipulations due to poor security.

It would be ideal if the OAIS model with its functional entities could be applied directly to a cloud environment, where services can be shared and abstracted in layers and where services such as storage and data management can be outsourced to a third-party and paid for on-the-fly. This could curb many integration challenges for legacy systems.

The study further recommends that organisations consider international standards and best practices outlined in section 6.4.4.2.2.

6.4.2 Records management expertise and stakeholders' involvement

This study recommends the development and occupation of records and archives management positions by professionally trained and skilled staff.

6.4.3 Choosing cloud services, deployment models and providers'

It did not come out clearly what influenced the decision to select the cloud computing services, and deployment models chosen for records management. The study recommends that clients do a comparison of cloud services, deployment models and providers before entering into contracts with cloud service providers to ensure that they provide all the necessary requirements in terms of infrastructure, security, skills, records management requirements, compliance with legal and regulatory framework and cost.

6.4.4 Framework for adopting cloud computing for records management in Namibia

The study proposes a framework for adopting cloud computing for records management in Namibia for both public and private entities.

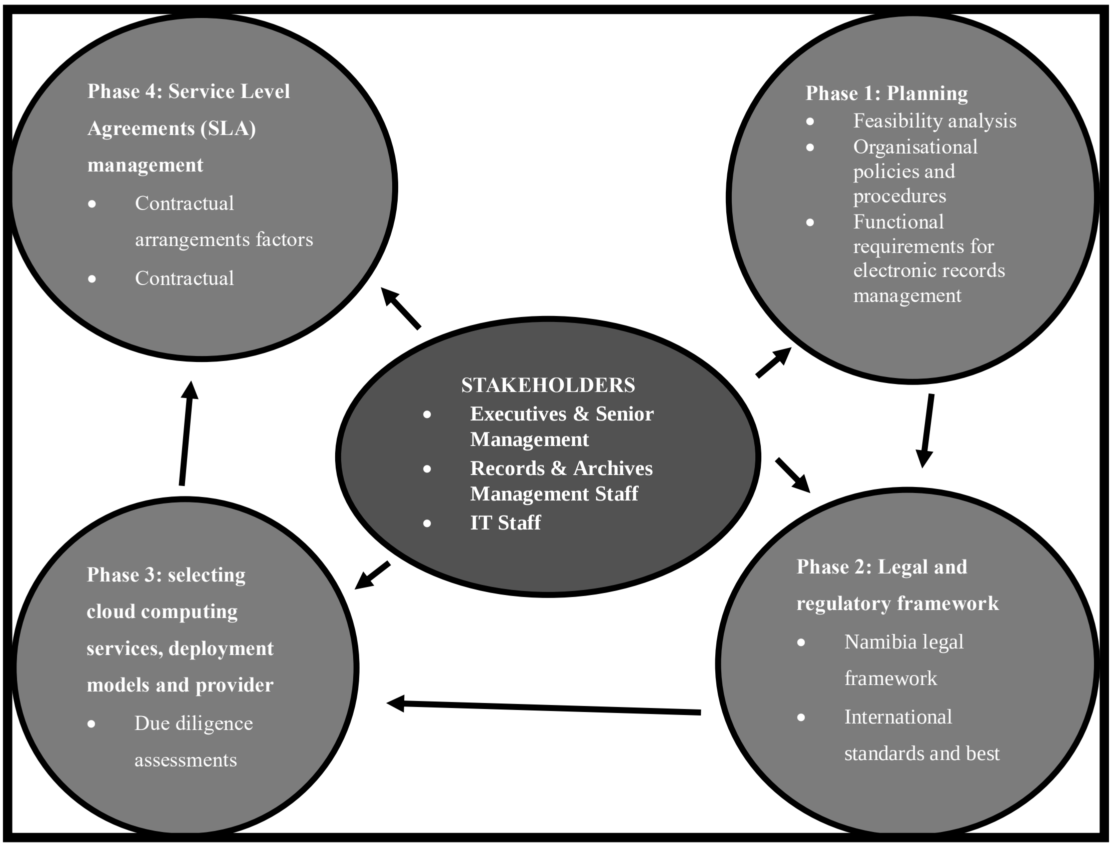

Phase 4: Service Level Agreements (SLA) management
• Contractual arrangements factors
• Contractual
Phase 1: Planning
• Feasibility analysis
• Organisational policies and procedures
• Functional requirements for electronic records management
STAKEHOLDERS
• Executives & Senior Management
• Records & Archives Management Staff
• IT Staff
Phase 3: selecting cloud computing services, deployment models and provider
• Due diligence assessments
Phase 2: Legal and regulatory framework
• Namibia legal framework
• International standards and best

Figure 6.1: Framework for adopting cloud computing for records management in Namibia

6.4.4.1 Phase 1: Planning

This phase consists of developing the knowledge on cloud computing and electronic records management practices. This can be achieved by conducting research, attending regional and international conferences, benchmarking locally and regionally, and networking to understand how cloud computing functions in different organisational structures, the benefits and risks, policies and the best usage practices of cloud computing. All the stakeholders need to be involved in this phase. Top management involvement will allow enough resources to be availed for the adoption of cloud computing, while collaboration among records managers, archivists and IT staff allows for a better understanding of electronic records management standards and functional requirements and how they should be considered in the usage of cloud computing for records management.

In this stage, the organisation should also develop or review organisational policies and procedures for the management of information. These policies and procedures should include records and archives management, and ICT policies and procedures. These policies and procedures should focus on user behaviour and address issues such as information confidentiality, integrity and access to information.

6.4.4.2 Phase 2: Legal and regulatory framework

6.4.4.2.1 Namibia legal and regulatory framework

The Archives Act 12 of 1992 and the Archives Code are Namibia's current main legislations on public records management. Compliance with these legislations is mandatory, especially for public institutions but not excluding private institution, as they do business with public entities. Another law related to electronic records management that should be complied with is the Electronic Transaction Act 4 of 2019, as electronic records emanating from electronic transactions need to be managed to remain trustworthy, authentic, have integrity and be accessible.

6.4.4.2.2 International standards and best practice

There are international standards for electronic records management that could influence the successful adoption of cloud computing to manage records, discussed in chapter 2. Such standards include:

- ISO 16175 - Principles and functional requirements for records in electronic office environments and MoReq2010 - Modular Requirements for Records Systems
- ISO 14721 – The Open Archival Information System Reference model (OAIS Reference model)

- Australian Digital Recordkeeping Initiative (ADRI) - Advice on Managing the Recordkeeping Risks associated with Cloud Computing.
- National Archives of Australia – A checklist for Records Management and the cloud
- Archives and Records Association - Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud

6.4.4.3 Phase 3: Selecting cloud computing services, deployment models and provider

Performing due diligence when selecting a cloud computing service, deployment model and provider is crucial to the success of using cloud computing to manage records. A comparison of cloud services, deployment models and providers needs to be done to establish the capability of complying with laws and standards, providing maximum security to records and ensuring long-term preservation for electronic records. Due diligence is a major responsibility of records managers, archivists and top management. Proper selection of cloud services, deployment model and provider is vital for electronic records management.

6.4.4.4. Phase 4: Service Level Agreements management

For the successful usage of cloud computing for records management, organisations should be able to negotiate contracts and agreements that fit their risk assessment and compliance requirements. It is important that any associated fees or service restrictions are fully documented to prevent organisations from being locked into underperforming service providers' contracts. All stakeholders should be involved in this phase.

6.5 Study findings implications for practice

The findings have culminated in the proposed framework (illustrated in Figure 6.1) consisting of four phases that should be addressed before an organisation commits to cloud computing for records management. The framework is flexible and it could be customised to suit any organisation. The framework aims to address the risks and challenges encountered in adopting cloud computing for electronic records management, and have a detriment effect on the integrity, reliability and usability of the records stored in the cloud. The framework could also inform policies on cloud computing for records management.

6.6 Recommendations for further research

The study identified the following areas for further research:

- Investigate the management of records in the cloud. Such a study can look into the implications of cloud computing for recordkeeping principles and standards and the development of cloud-specific guidelines and policies.
- One of the risks of managing records in the cloud is failure to access records if hardware and software obsolesce is not addressed. A study could investigate cloud computing implications for the long-term preservation of records in the cloud.
- This study concentrated on Namibia’s private organisations, leaving out the public sector. Future research can be done to establish the impact of cloud computing on records management in the public sector.
- A lack of collaboration among records managers, archivists and IT professionals in the designing and adoption of cloud computing for records management was identified by this study. Further research could investigate the nature of collaboration necessary among these professionals for the successful adoption of cloud computing for records management.

6.7 Final conclusion

There are benefits to be realised from adopting cloud computing for records management. Similarly, there are risks that organisations need to be aware of. There are mitigating factors an organisation can take to lead to fully realise cloud computing benefits for records management. Such factors include compliance to legal and regulatory framework, and collaboration of IT and skilled records and archives management staff.

REFERENCES

African Union. (2022). *Namibia review report: Key highlights*. African Peer Review Mechanism. https://www.aprm-au.org/wp-content/uploads/2022/02/Namibia-Key-Highlights-design.pdf

Alrowaihi, H.S. (2014). Understanding the cloud: Towards a suitable cloud service. *International Journal of Scientific and Research Publications*, *4*(*1*), 1-6. https://www.academia.edu/11434130/Understanding_the_Cloud_Towards_a_Suitable_Cloud_Service?auto=download

Asogwa, B.E. (2012). The challenge of managing electronic records in developing countries: Implications for records managers in sub Saharan Africa. *Records Management Journal 22*(3), 198–211. https://doi.org/10.1108/09565691211283156

Askhoj, J., Sugimoto, S., & Nagamori, M. (2011). Preserving records in the cloud. *Records Management Journal 21*(3), 175-187. doi.10.1108/09565691111186858

Barata, K., Bennett, R., Cain, P., & Routledge, D. (2001). *From accounting to accountability: managing financial records as a strategic resource: Namibia: A case study*. London: International Records Management Trust.

Barnes, F. R. (2010). Putting a lock on cloud-based information: collaboration between records and IT professionals before contracting with cloud-based information services will help organisations ask the right questions to ensure their information is secure. *Information Management Journal*, *44*(4), 26–30. https://web-s-ebscohost-com.ezproxy.unam.edu.na/ehost/pdfviewer/pdfviewer?vid=1&sid=67fce76e-777c-4dd9-980b-d2fb762b5b50%40redis

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels in organisational research. *Human Relations* *61*(8), 1139-1160. doi: 10.1177/0018726708094863

Bassett, C. (2015). *Cloud computing and innovation: Its viability, benefits, challenges and records management capabilities.* Unpublished master's thesis, University of South Africa, Pretoria Gauteng, South Africa. https://core.ac.uk/download/pdf/43178115.pdf

Beagrie, N., Charlesworth, A., & Miller, P. (2014). *Guidance on Cloud Storage and Digital Preservation: How Cloud Storage can address the needs.* The National Archives. UK. https://cdn.nationalarchives.gov.uk/documents/CloudStorage-Guidance_March-2015.pdf

Bernbom, G., Lippincott, J., & Eaton, E. (1999). Working Together: New Collaborations among Information Professionals. *CAUSE/EFFECT journal, 22*(2). https://www.educause.edu/ir/library/html/cem/cem99/cem9922.html

Blanche, M. T., Durrheim, K., & Kelly, K. (2006). First steps in qualitative data analysis. In M. T. Blanche, K. Durrheim, & D. Painter (Eds.), *Research in practice: Applied methods for social sciences* (2nd. ed., pp. 321-344). Cape Town.

Bless, C., Sithole L., & Higson-Smith, C. (2013). *Fundamentals of social research methods: An African perspective* (5th ed.). Cape Town: Juta.

Bricki, N., & Green, J. (2007). *A guide to using qualitative research methodology*. London School of Hygiene and Tropical Medicine. https://fieldresearch.msf.org/handle/10144/84230

Bui, Y.N. (2009). How to write a master's thesis. London: SAGE.

Burton, D. (Ed.). (2000). *Research training for social scientists: A handbook for postgraduate researchers*. London, United Kingdom: Sage.

Carroll, M., Van der Merwe, A., & Kotzé, P. (2011). Secure cloud computing: Benefits, risks and controls. Conference Paper. *Information security for South Africa*. doi: 10.1109/ISSA.2011.6027519

Centre for Internet Security (CIS). (2021). *Shared Responsibility for Cloud Security: What You Need to Know.* [online]. https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know

Chitauro, S. (2017). *Designing a cloud based e-learning implementation model for higher and tertiary institutions in Namibia.* Unpublished master thesis, Namibia University of Science and Technology, Windhoek, Namibia. http://ir.nust.na/bitstream/handle/10628/602/Shadreck%20Chitauro%20201001003%20Final%20Masters%20Thesis.pdf?sequence=1&isAllowed=yhttp://ir.nust.na/bitstream/handle/10628/602/Shadreck%20Chitauro%20201001003%20Final%20Masters%20Thesis.pdf?sequence=1&isAllowed=y

Cloud Security Alliance. (2012). *SecaaS implementation guidance: Business continuity and disaster recovery*. https://downloads.cloudsecurityalliance.org/initiatives/ secaas/SecaaS_Cat_9_BCDR_Implementation_Guidance.pdf

Cloud Security Alliance. (2020). *Shared Responsibility Model Explained.* https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

Cloud Standards Customer Council. (2017). *Cloud standards customer council announces version 3.0 of practical guide to cloud computing*. Business Wire.

https://www.businesswire.com/news/home/20171205005186/en/ Cloud-Standards-Customer-Council-Announces-Version-3.0.

Convery, N. (2010a). *Cloud computing toolkit: Guidance for outsourcing information storage to the cloud*. Department of information studies, Aberystwyth University, UK. http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

Convery, N. (2010b). *Storing information in the cloud: Project report*. Department of information studies, Aberystwyth University, UK. http://www.archives.org.uk/images/documents/Cloud_computing_report_final-1.pdf

Council of Australian Archives and Records Authority (CAARA). (2010). *Advice on managing the recordkeeping risks associated with cloud computing.* Australia: Australasian Digital Recordkeeping Initiative (ADRI). http://www.sro.wa.gov.au/sites/default/files/adri_cloud_computing.pdf

Corrado, E. M. & Moulaison, H. L. (2015). Digital preservation and the cloud: Challenges and Opportunities. I*FLA 2015 Preconference satellite meeting preservation & conservation Section*, 12-13 August, Durban, South Africa. https://www.researchgate.net/publication/304214940_Digital_preservation_and_the_cloud_Challenges_and_opportunities

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches.* (2nd Ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2007). *Qualitative inquiry and research design: choosing among five approaches* (2nd Ed). Thousand Oaks, CA: Sage

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods Research*, (2ND Ed.) Thousand Oaks, LA: Sage.

Creswell, J.W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th Ed.). Thousand Oaks, CA: Sage.

Diaby, T., & Rad, B.B. (2017). Cloud computing: A review of the concepts and deployment models. *International Journal of Information Technology and Computer Science 9*(6): 50-58. doi: 10.5815/ijitcs.2017.0607

David, M., & Sutton, C.D. (2011). *Social research: An introduction* (2nd ed.). London: Sage.

Duis, E. (2014). *The involvement of records managers in cloud computing decisions: A cross-sectional study of New Zealand records managers.* Unpublished Master thesis, Victoria University of Wellington, New Zealand). https://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/3398/thesis.pdf?sequence=2

Duranti, L., & Jansen, A. (2013). Records in the cloud: authenticity and jurisdiction. Paper presented at the Digital Heritage International Congress, France. https://www.researchgate.net/publication/271552900_Records_in_the_Cloud_Authenticity_and_jurisdiction

Durrheim, K. (2006). Research design. In M. T. Blanche, K. Durrheim, & D. Painter (Eds.), *Research in practice: Applied methods for social sciences* (2nd ed.), 33-59. Cape Town, Juta.

Fahmideh, M., Daneshgar, F., Beydoun, G., & Rabhi, F. (2017). Challenges in migrating legacy software systems to the cloud—an empirical study. *Information Systems journal 6*(7), 100-113. doi: 10.1016/j.is.2017.03.008.

Farguhar, J. D. (2012). *Case study research for business*. Thousand Oaks: Sage.

Farrell, R. (2010). Securing the cloud-governance, risk, and compliance issues reign supreme. *Information Security Journal: A Global Perspective, 19*(6), 310–319. doi.10.1080/19393555.2010.514655

Ferguson-Boucher, K. (2011). Cloud computing: A records management perspective. *IEEE Computer and Reliability Societies,* *9*(6): 63-66. doi: 10.1109/MSP.2011.159.

Gaur, A., Gaud, S., & Jain, A. (2017). Advance Computing Paradigm with the Perspective of Cloud Computing - An Analytical Study. *International Journal of Advanced Networking and Applications,* *8*(*6*), 3257-3265. https://www.ijana.in/papers/V8I6-5.pdf

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal, 204*(6), 291 – 295. doi: 10.1038/bdj.2008.192

Goldin, M. (2017). *Data security and the cloud: Earn trust by putting your customers in control: It's not your data; it's the customer's data*. InfoWorld, United States. https://www.infoworld.com/article/3187725/data-security-and-the-cloud-earn-trust-by-putting-your-customers-in-control.html

Gomm, R. (2009). *Key concepts in social research methods*. England, United Kingdom: Palgrave Macmillan.

Gorelik, E. (2013). *Cloud computing models.* Unpublished master thesis, Massachusetts Institute of Technology, Cambridge. http://web.mit.edu/smadnick/www/wp/2013-01.pdf

Government of South Australia, State Records of South Australia (2015). *Cloud computing and records management guideline.* Adelaide, South Australia: Author.

https://government.archives.sa.gov.au/sites/default/files/20150706%20Cloud%20Computing%20and%20Records%20Management%20Final%20V1.pdf

Gray, D. E. (2009). *Doing research in the real world* (2nd ed.). London, United Kingdom: Sage.

Hainaut, J.L., Cleve, A., Henrard, J., & Hick, J-M. (2008). Migration of legacy information systems. In: T. Mens Tom & S. Demeyer (Eds.), *Software evolution* (pp. 105-138). Springer.

Heriot Watt University. (2017). *University research ethics policy*. Edinburgh, Scotland: Author. https://www.hw.ac.uk/documents/research-ethics-policy.pdf

Hess, R. (2004). How to write an effective discussion. https://cancer.dartmouth.edu/documents/pdf/effective_discussions.pdf

Hidalgo, J.R. (2013). *How Cloud Computing (SaaS) Supports an Electronic Document and Records Management System (EDRMS)*. Unpublished master thesis, University of Oregon, USA. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/19749/Hidalgo2013.pdf

International Records Management Trust. (1999a). *The management of public sector records: Principles and context.* London: Author. https://www.irmt.org/documents/educ_training/public_sector_rec/IRMT_principles.pdf

International Records Management Trust. (1999b). *Managing Electronic Records.* London: Author. https://www.irmt.org/documents/educ_training/managing electronic rec/IRMT_principles.pdf

International Records Management Trust. (2009). *Glossary of terms*. London: Author. https://www.irmt.org/documents/educ_training/term%20modules/IRMT%20 TERM%20Glossary%20of%20Terms.pdf

International Research on Permanent Authentic Records in Electronic Systems (InterPARES). (2006). *Terminology Database*. Canada: author. www.interpares.org/ip2/ip2_terminology_db.cfm

International Research on Permanent Authentic Records in Electronic Systems (InterPARES). (2018). *Investigating the management of digital records in enterprise-wide systems:* InterPARES Trust Project. Botswana. https://interparestrust. org/assets/public/dissemination/AF04_FinalReport_July2018.pdf.

International Organisation for Standards. (2016). ISO 15489-1 information and documentation - records management - part 1: concepts and principles. Geneva, Switzerland: Author. https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en

International Organisation for Standards. (2019). *ISO 22301: Security and resilience — Business continuity management systems — Requirements.* Geneva, Switzerland: Author. https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

Iron Mountain. (2020). *The Impact of Covid-19 on Records and Information Management (RIM).* Publisher. https://www.ironmountain.com/resources/infographics-and-tools/t/the-impact-of-covid-19-on-records-and-information-management.

IST-Africa. (2014). *Overview of ICT Infrastructure in Namibia*. Africa: author. http://www.ist-africa.org/home/default.asp?page=doc-by-id&docid=3581

IST-Africa. (2018). *Report on ICT Initiatives, Research and Innovation Priorities and Capacity in IST-Africa Partner Countries*. Africa: author. http://www.ist-africa.org/home/files/IST-Africa_D2.1_ ICTInitiatives_ResearchInnovationPriorities_ v2_Dec18.pdf

Jacobs, L.C. (2014). The research report. In F. Du Plooy-Cilliers. C. Cronje, & R. M Bezuidenhout (Eds.), Research matter (pp. 294- 309). Cape Town, South Africa: Juta and Company.

Jadeja, Y., & Modi, K. (2012). 'Cloud computing – concepts, architecture and challenges' in IEEE (Institute of Electrical and Electronics Engineers). *International Conference on Computing, Electronics and Electrical Technologies*. Nagercoil, Tamil Nadu, India, 21-22 March. New York: Curran Associates. https://www.researchgate.net/publication/254035330_Cloud_computing_-_concepts_architecture_and_challenges/link/545715880cf26d5090a97114/download

Kabata, V. (2012). Outsourcing records storage to the cloud: Challenges and prospects for African records managers and archivists. *Sabinet African Journals 30*(2), 137–157. doi: 10.10520/EJC144285

Kelly, K. (2006). From encounter to text: Collecting data in qualitative research. In: M.T. Blanche, K. Durrheim, & D. Painter (Eds.), *Research in practice: Applied methods for social sciences* (2nd ed.). 285-319. Cape Town, Juta.

Kibe, L. (2016, August). Impact of cloud-based services on records management in public organisations in Kenya. *Paper presented at the first International conference on Information and Knowledge Management,* Nairobi.

https://www.researchgate.net/publication/307569275_Impact_of_cloud_based_services_on_records_management

King, T. (2019). *Data Management vs. Content Management; What's the Difference?* Solution review. https://solutionsreview.com/data-management/data-management-vs-content-management-whats-the-difference/

Leedy, P.D., & Ormrob, J.E. (2010). *Practical research: Planning and design* (9th ed.). New York City: Merril.

Lewis-Beck, M. S., Bryman, A., & Liao, F. T. (2004). Interview guide. *The SAGE encyclopedia of social science research methods 1*(0). Thousand Oaks: Sage. doi: 10.4135/9781412950589

Liamputtong, P., & Ezzy, D. (2005). *Qualitative research methods* (2nd ed.). South Melbourne: Oxford University Press.

Long, R. (2020). *COVID-19: Records Management as a Function of Business Continuity*. [online]. https://www.feith.com/coronavirus-records-management/.

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

MacNeil, H. (2000). Providing grounds for trust: developing conceptual requirements for long-term preservation of authentic electronic records. *Archivaria 50*(Fall):52–78. https://archivaria.ca/index.php/archivaria/article/view/12765/13955

Marker, A. (2022). *Audit Trails: Managing the Who, What, and When of Business Transactions.* Smatsheet, USA. https://www.smartsheet.com/audit-trails-and-logs

Marutha, N. S., & Ngulube, P. (2012). Electronic records management in the public health sector of the Limpopo provenance in South Africa. *Journal of the South African Society of Archivists, 45:* 39-67. https://www.ajol.info/index.php/jsasa/article/view/85723/75632

Masud, A. H., & Huang, X. (2012, May). Cloud computing for higher education: A roadmap. *Paper presented at the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design*. Wuhan, China. doi: 10.1109/CSCWD.2012.6221872

Matangira, V. (2016). Records and archives management in postcolonial Zimbabwe's public service. Unpublished doctoral dissertation. University of Namibia, Windhoek, Namibia. Windhoek. https://repository.unam.edu.na/bitstream/handle/11070/1644/Matangira_2016.pdf?sequence=1&isAllowed=y

McDade, M. (2022). What are the security risks of cloud computing? *Expert Insight, US.* https://expertinsights.com/insights/what-are-the-security-risks-of-cloud-computing/#:~:text=Data%20Security%20%2F%20Privacy&text=Risks%20to%20data%20hosted%20on,malicious%20activities%20(hacking%20or%20viruses)

McLeod, J., & Gormly, B. (2017). Using the cloud for records storage: issues of trust. *Archival Science Journal*, *17*(4), 349-370. doi: 10.1007/s10502-017-9280-5

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. Gaithersburg, Maryland: National Institute of Standards and Technology.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Miles, M.B., & Huberman, A.M. (1994). *Qualitative data analysis* (2nd ed.). Thousand Oaks: Sage.

Ministry of Information and Communication Technology. (2017). *Strategic plan 2017-22.* Namibia: author. http://www.mict.gov.na/documents/32978/266786/MICT+STRATEGIC+PLAN+2017-2022/3596bd32-0aa5-498a-b4c9-b396af9e8c1a

Mohamed, A.M., & Pillutla, S. (2014). Cloud computing: a collaborative green platform for the knowledge society. VINE Journal of Information and Knowledge Management Systems 44(3), 357-374. doi: 10.1108/VINE-07-2013-0038

Mosweu, T.L. (2012). Assessment of the court records management system in the delivery of justice at the Gaborone Magisterial District. Unpublished MA thesis, University of Botswana, Gaborone.

Mosweu, T., Luthuli, L., & Mosweu, O. (2019). Implications of cloud-computing services in records management in Africa: Achilles heels of the digital era? *South African Journal of Information Management, 21*(10), 1-12. doi: 10.4102/sajim.v21i1.1069

Mugyenyi, R. (2018) Adoption of cloud computing services for sustainable development of commercial banks in Uganda. *Global Journal of Computer Science and Technology: B Cloud and Distributed 18*(1), 1–10. doi: 10.17406

Mutula, S. (2008). Digital divide and economic development: Case study of sub-Saharan Africa. *The Electronic Library 26*(4), 468–489. doi:10.1108/02640470810893738

Namibia Internet Governance Forum (NamIGF). (2017). *Namibia Internet Governance Forum 2017 report*. Namibia: author. https://action-namibia.org/wp-content/uploads/2018/11/Nam-IGF-Report-2017.pdf

Namibia Internet Governance Forum (NamIGF). (2021). only half of Namibia's population has access to the internet. Namibia Economist. https://economist.com.na/66397/technology/only-half-of-namibias-population-has-access-to-the-internet/

National Archives of Australia. (2018). *Business continuity and disaster planning*. http://www.naa.gov.au/information-management/managing-information-and records/protecting/business-continuity/index.aspx.

National Institute of Standards and Technology (NIST). (2011). *Guidelines on security and privacy in public cloud computing*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Nengomasha, C. T. (2009). *A study of electronic records management in the Namibian Public Service in the context of e-government*. Unpublished doctoral dissertation. University of Namibia, Windhoek, Namibia. http://repository.unam.edu.na/bitstream/handle/11070/447/nengomasha2009.pdf?sequence=1&isAllowed=y

Neuman, W.L. (2014). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Boston: Pearson.

New South Wales Government State Record. (2012). *FAQs about EDRMS*. http://www.records.nsw.gov.au/recordkeeping/advice/designingimplementing-and managing-systems/faqs-about-edrms#what-is-an-edrms-

Ncaagae-Mbe, K. (2021). Managing Records in the Covid-19 Era at the Botswana Communications Regulatory Authority. *Mousaion: South African Journal of Information Studies, 39* (4),12-25. doi: 10.25159/2663-659X/9976.

Nghihalwa, E., & Shava, B. F. (2018). *An Assessment of cloud computing readiness in the Namibian government's information technology departments*. Windhoek: Namibia University of Science and Technology (NUST). https://ieeexplore.ieee.org/document/8379074

Ngoepe, M., & Saurombe, A. (2016). Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African development community. *Archives and Manuscripts 44*(1), 24–41. doi: 10.1080/01576895.2015. 1136225

Nieuwenhuis, J., & Smit, B. (2012). Qualitative research. In C. Wagner, B. Kawulich, & M. Garner (Eds.), (2012). *Doing social research: A global context* (pp. 124-139). Berkshire, United Kingdom: McGraw Hill.

Office of the President. (2004). Namibia vision 2030. Republic of Namibia. https://www.npc.gov.na/vision-2030/

Office of the Prime Minister. (2019). *Electronic Transactions Act 4 of 2019.* Republic of Namibia. https://www.lac.org.na/laws/annoSTAT/Electronic%20Transactions%20Act% 204%20of% 202019.pdf

O'Keeffe, V. (n.d.). *Jurisdictional issues associated with a move to the cloud.* Cork Institute of Technology. [online]. https://www.academia.edu/6174499/Jurisdictional_issues_associated_with_a _move_to_the_Cloud

Oppenheim, C. (2012). *The no-nonsense guide to legal issues in web 2.0 and cloud computing*. London: Facet.

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). London: Sage.

Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). London: Sage.

Prasath, T., Gnanaraj, R.P.J., & Ganesh, K.S. (2013). A generalized approach on cloud computing. *International Journal for Scientific Research & Development 1*(10), 2228-2230. http://www.ijsrd.com/articles/IJSRDV1I10043.pdf

Punch. K.F. (2005). *Introduction to social research: Quantitative and qualitative approaches* (2nd ed). London: Sage.

Puthal, D., Sahoo, B.P.S., Mishra, S., & Swain, S. (2015). *Cloud computing features, issues, and challenges: A big picture*. Paper presented at the International Conference on Computational Intelligence and Networks, India. doi: 10.1109/CINE.2015.31

Rao C., Leelarani, M., & Kumar, R. (2013). Cloud Computing services and deployment models. *International Journal of Engineering and Computer Science, 2*(*12*), 3389-3392. http://www.ijecs.in/index.php/ijecs/article/view/2254

Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: A brief review. *International Journal of Computer Science and Engineering 7*(*2*), 421-426. doi: 10.26438/ijcse/v7i2.421426

Ravanbakhsh, A. D. (2010). *NARA's FAQ and bulletin on managing federal records in cloud computing environments*. Paper presented at the Records administration conference, Chicago. https://www.archives.gov/files/records-mgmt/presentations/ravanbakhsh.ppt

Rice, E. (2022). *The relationships between data, information, and records.* Texas Record. https://www.tsl.texas.gov/slrm/blog/2022/05/the-relationships-between-data-information-and-records/

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud computing implementation, management and security*. New York, CRC Press. f

Robinson, B. (2010). *What you need to know about storage in the cloud.* Federal Computer Week. https://fcw.com/it-modernization/2010/04/what-you-need-to-know-about-storage-in-the-cloud/222799/

Romeo, C. (2020). *6 ways to develop a security culture from top to bottom.* TechBeacon. United States. https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

Rosencrance, L. (2020). *Breaking Down the Cost of Cloud Computing.* Tech Target. https://www.techtarget.com/whatis/Breaking-Down-the-Cost-of-Cloud-Computing

Rountree, D., & Castrillo I. (2013). *The basics of cloud computing: Understanding the fundamentals of cloud computing in theory and practice*. doi: 10.1016/C2012-0-02521-5

Runardotter, M. (2007). *Information Technology, Archives and Archivists: An Interacting Trinity for Long-term Digital Preservation.* Unpublished licentiate thesis, Luleå University of Technology, Lulea, Sweden. https://www.diva-portal.org/smash/get/diva2:990565/FULLTEXT01.pdf

Schneider, T. K. (2021). *The long road to electronic records management.* FCW. https://fcw.com/it-modernization/2021/02/the-long-road-to-electronic-records-management/258692/

Sen, J. (2015). Security and privacy issues in cloud computing. In Information Resources Management Association (IRMA) (Ed), *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (p. 46). Kolkata, India.

Silverman, D. (2000). *Doing qualitative research: A practical handbook*. London: Sage.

Somepalle, S. (2015). *3 Service and 4 deployment models of cloud computing.* Model N. https://www.linkedin.com/pulse/3-service-4-deployment-models-cloud-computing-sankar-somepalle/

State Archives of North Carolina. (2013). *Guidelines for managing trustworthy digital public records.* Raleigh, North Carolina, United States: Author. https://files.nc.gov/dncr-archives/documents/files/guidelines_for_digital_public_records.pdf

Stedman, C., & Vaughan, J. (2020). *What is data management and why is it important?* Tech Target. https://www.techtarget.com/searchdatamanagement/definition/data-management

Stuart, K., & Bromage, D. (2010). Current state of play: Records management and the cloud.*Records Management Journal, 20* (2), 217-225, doi: 10.1108/09565691011064340

Takabi, H., Joshi, J.B.D., & Ahn, G.J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy* 8(6), 24-31. doi: 10.1109/MSP.2010.186

Taylor-Powell, E. & Steele, S. (1996). *Collecting evaluation data: Direct observation*. University of Wisconsin-Extension. Cooperative Extension publication, 201 Hiram smith hall. https://ucanr.edu/sites/CEprogramevaluation/files/294189.pdf

Thomas, G. (2011). *How to do your case study: A guide for students and researchers*. London: Sage.

Tjikongo, R., & Uys, W. (2013, January). *The viability of cloud computing adoption in SME's in Namibia.* Paper presented at the IST-Africa Conference and Exhibition, Nairobi, Kenya. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6701756

Tolliver-Nigro, H. (2009). SaaS 101: The basics of software as a service. The Seybold report: *Analyzing Publishing Technologies, 9*(15), 3–8. https://web-p-ebscohost-com.ezproxy.unam.edu.na/ehost/pdfviewer/pdfviewer?vid=0&sid=8fb8cafb-fe60-475d-9a81-ab47d666b61d%40redis

Wamuyu, P.K. (2017). Use of cloud computing services in micro and small enterprises: A fit perspective. *International Journal of Information Systems and Project Management, 5*(2), 59–81. doi: 10.12821/ijispm050204

Wassenaar, D. R. (2006). Ethical issues in social science research. In: M. T. Blanche, K. Durrheim, & D. Painter (Eds.), *Research in practice: Applied methods for social sciences* (2nd. ed., pp. 60-79). Cape Town, Juta.

Yimam, D., & Fernandez, E. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications, 7* (1). doi: 10.1186/s13174-016-0046-8

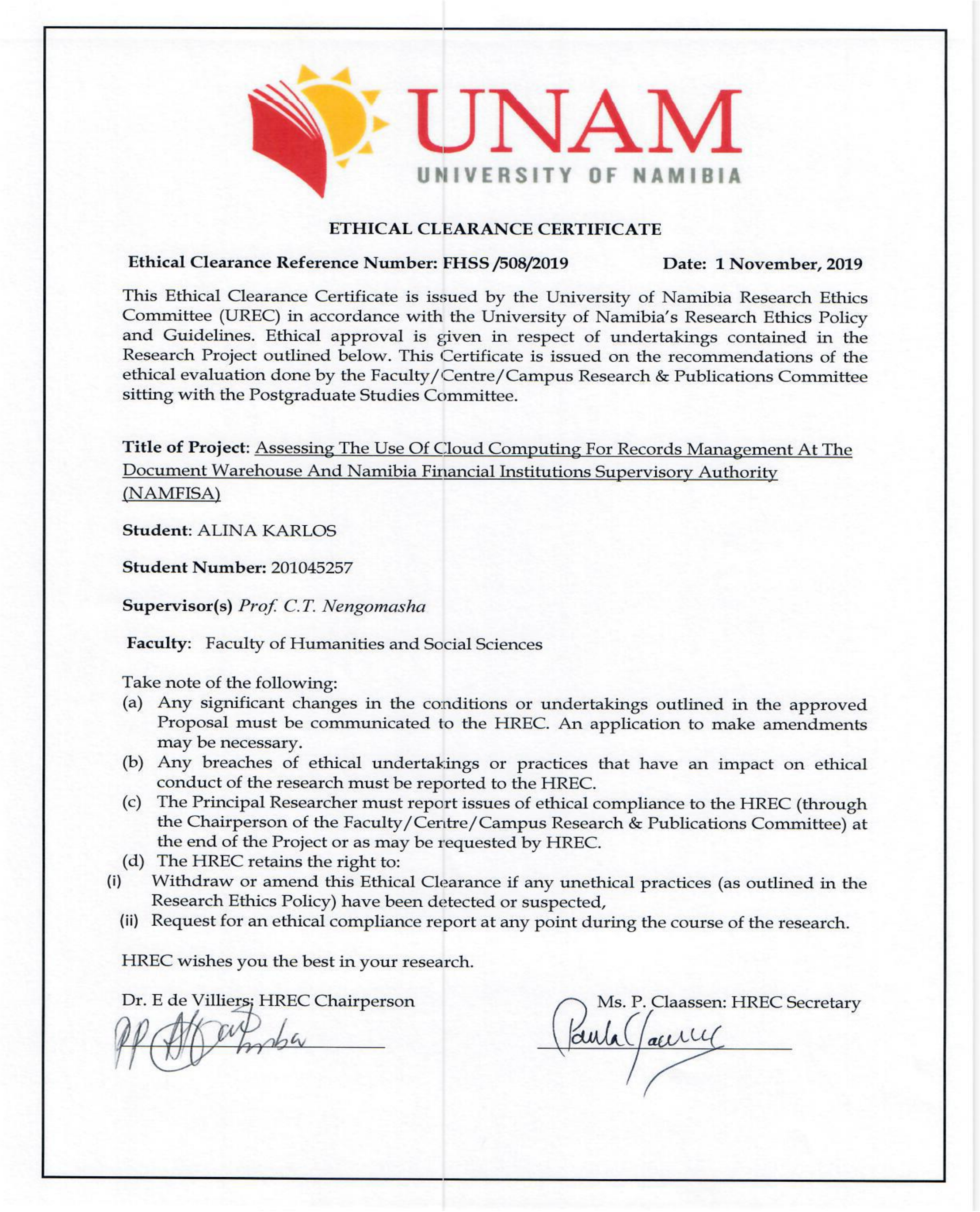
Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Applied social research methods series vol.5. Thousand Oaks: Sage.

Youssef, A. E. (2012). Exploring cloud computing services and applications. *Journal of Emerging Trends in Computing and Information Sciences* 3(6), 838-847. https://www.researchgate.net/publication/299559183_Exploring_Cloud_Computing_Services_and_Applications

Zalazar, A. S., Gonnet, S., & Leone, H. (2015). Migration of legacy systems to cloud computing. *SADIO Electronic Journal of Informatics and Operations Research*, *14*(1), 42-55. http://www.sadio.org.ar/wp-content/uploads/2016/04/EJS_14_Paper_3.pdf

APPENDICES A - F

APPENDIX A: ETHICAL CLEARANCE



UNAM
UNIVERSITY OF NAMIBIA

ETHICAL CLEARANCE CERTIFICATE

Ethical Clearance Reference Number: FHSS /508/2019 **Date: 1 November, 2019**

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: Assessing The Use Of Cloud Computing For Records Management At The Document Warehouse And Namibia Financial Institutions Supervisory Authority (NAMFISA)

Student: ALINA KARLOS

Student Number: 201045257

Supervisor(s) *Prof. C.T. Nengomasha*

Faculty: Faculty of Humanities and Social Sciences

Take note of the following:

(a) Any significant changes in the conditions or undertakings outlined in the approved Proposal must be communicated to the HREC. 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 HREC.

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

(d) The HREC 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.

HREC wishes you the best in your research.

Dr. E de Villiers: HREC Chairperson

Ms. P. Claassen: HREC Secretary

APPENDIX B: LETTER SEEKING PERMISSION TO CARRY OUT RESEARCH

29 June 2020

To Whom It May Concern

Re: Requesting your participation in Ms Alina Karlos' Research

We wish to introduce to you Ms Alina Karlos, an MA in Records and Archives Management candidate in the Department of Information and Communication Studies, University of Namibia. Her research project is titled "Assessing the Use of Cloud Computing for Records Management in selected Namibian orgainsations". We are requesting your assistance by participating in Ms Karlos' study.

We rely on the support of you our stakeholders for the success of our programmes. Thank you in advance for your support.

Yours Sincerely,

CNengomasha

Prof C.T. Nengomasha

Supervisor, Department of Information and Communication Studies

Cell: 0812787617; Office: 2063641; email: cnengomasha@unam.na

APPENDIX C: INFORMED CONSENT FORM

UNAM
UNIVERSITY OF NAMIBIA

TITLE OF THE RESEARCH PROJECT: Assessing the use of cloud computing for records management in selected Namibian organisations

REFERENCE NUMBER: 201045257

PRINCIPAL INVESTIGATOR Alina Karlos

ADDRESS Private bag 13301, Pionierspark, Windhoek

CONTACT NUMBER +264613692 / +264817426356

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. Please ask the study staff or doctor any questions about any part of this project that you do not fully understand. 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?

The study will be conducted at four Organisations in Windhoek offices. The study will involve eight (less or more) participants, two (less or more) from each organisation, representing IT and records management staff respectively.

The study aims to investigate and assess the use of cloud computing for records management in Namibia. The significance of this study is that it could be used to inform policy formulations and act as a guide for organisations planning to adopt cloud computing for records management.

The researcher will obtain a research permission letter from the School of Postgraduate studies at UNAM and authorisation to conduct the study in the organisations. Participants will sign informed consent forms and interviews will take approximately 45 minutes. The data will be collected at the four Organisations at their Windhoek office premises, at the participant's offices. Observations will be done concurrently with interviews.

2. **Why have you been invited to participate?**

You have been invited to participate in the study because of your direct involvement with records management and cloud computing.

3. **What will your responsibilities be?**

Your responsibility is to answer interview questions as honestly as you most possibly can, unless you opt to not answer particular questions. In addition, you will be required to provide the investigator with documentations and processes in place for cloud computing as presented in the observation checklist.

The interview will take approximately 45 minutes.

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

As a participant, you will gain new knowledge on cloud computing for records management and your organisation will benefit from the overall study as a guide to policy formulation or review.

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

   For this study, the participant is free to not agree to be part of the research or to withdraw at any time with no consequences.

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

   This study is for academic degree purpose, there are no payments for taking part in this study.

7. **Is there anything else that you should know or do?**

a) *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.*

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

8. **Declaration by participant**

   By signing below, I ………………………………..……….. agree to take part in a research study entitled *Assessing the use of cloud computing for records management in Namibia.*

   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 may be asked to leave the study before it has finished, if the study doctor or researcher feels it is in my best interests, or if I do not follow the study plan, as agreed to.

Signed at (*place*) ....…........……………….. on (*date*) …………...……….. 2019.

.. **..**

Signature of participant Signature of witness

9. Interview recording agreement

By signing below, I ……………………………………………….. agree to give permission for my interview to be recorded by the investigator for the purpose of this study.

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

10. Declaration by investigator

I Alina Karlos 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/did not use an interpreter.

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

.. **...**

Signature of investigator Signature of witness

APPENDIX D: INTERVIEW GUIDE FOR IT STAFF: CLOUD COMPUTING PROVIDER

Instructions: Everything in bold is for the attention of the interviewer and not to be read out to the interviewee.

Interviewer introduce him/herself.

Interviewer hand over the consent form to the interviewee to sign.

a) Please briefly introduce yourself

b) Please briefly explain the work you do here?

c) How long have you been working here?

1. Reasons for adopting cloud computing for records management.

a) I understand your organisation is a cloud service provider, briefly explain what you understand of 'cloud computing for records management'?

b) What are the total costs of setting up and managing cloud services?

2. Cloud computing services and deployment models.

a) Which service(s) do you provide for records management?

b) Which deployment model(s) do you provide for records management?

c) Does the client have different service and deployment models to choose from?

d) What are the reasons behind providing those particular service(s) and deployment model(s) for records management?

e) What are the organisation's responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

3. The benefits of cloud computing for records management.

a) What are the potential benefits for your clients using cloud computing for records management?

4. Risks of managing records in the cloud.

a) What are the challenges and risks associated with cloud computing?

b) How do you as a provider protect information and systems against unauthorised access (hacking, interruption, loss, etc.)?

c) What is the impact of outsourcing services and information to the cloud on the organisation's legislative and regulatory requirements?

d) How will an organisation be able to negotiate contracts and agreements that fit its risk assessment and compliance environment?

e) What is the physical location of the data centre where records are stored?

5. Measures to mitigate risks of managing records in the cloud.

a) How are your clients' security considerations addressed in the Service Level Agreement (SLA)?

b) How can your clients be assured of the integrity, authenticity, and reliability of information stored in the cloud?

c) How can your clients apply their records and information management programs to the cloud environment (retention schedules)?

d) How does your clients audit and monitor cloud services and establish relevant service-level agreements?

e) To what extent is cloud computing a viable option for records management?

Last Question: Do you have any other comments about the use of cloud computing for records management?

This is all I had to ask you. Is there anything you would like to ask me or comment about this interview? Thank you for your time and contribution to this research.

End of interview

APPENDIX E: INTERVIEW GUIDE FOR IT STAFF: CLOUD COMPUTING CLIENT

Instructions: Everything in bold is for the attention of the interviewer and not to be read out to the interviewee.

Interviewer introduce him/herself.

Interviewer hand over the consent form to the interviewee to sign.

d) Please briefly introduce yourself

e) Please briefly explain the work you do here?

f) How long have you been working here?

6. Reasons for adopting cloud computing for records management.

a) I understand your organisation is using cloud computing for records management, briefly explain your understanding of cloud computing?

b) Who was involved in making the decision to use cloud computing for records Management?

c) What are the reasons that led to the adoption of cloud computing for records management?

d) Which system(s) were used for records management before adopting cloud computing? **[ask for a demonstration / documentations of the system(s)]**

e) How are the previous systems integrated into the cloud computing solution adopted?

f) Is there a cloud computing implementation policy document? [**If yes, ask for copy. If no, ask what is used to guide the implementation of cloud computing].**

7. Cloud computing services and deployment models.

a) Which service model(s) is your organisation using? **[ask for a demonstration / documentations of the services model(s)]**

b) Which deployment model(s) is your organisation using? **[ask for a demonstration / documentations of the deployment model(s)]**

c) What are the organisation's responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

8. Factors to consider when choosing a cloud service provider, service and deployment model(s).

a) Who was involved in deciding which cloud computing service(s) and deployment model(s) to use?

b) What are the reasons for choosing that service(s) and deployment model(s)?

c) Why did you choose that cloud service provider?

d) How do you collaborate with your records management department on cloud computing and to what extend?

9. The benefits of cloud computing for records management.

a) What are the benefits of cloud computing your organisation is experiencing?

b) To what extent is cloud computing a viable option for records management?

10. Risks of managing records in the cloud.

a) What are the challenges and risks associated with managing records in the cloud?

b) How does the provider protect information and systems against unauthorised access (hacking, interruption, loss, etc.)?

c) Which security standards are supported by the cloud computing solution adopted?

d) Is there a security policy for cloud computing? **[if yes, request for a copy]**

e) What is the impact of outsourcing services and information to the cloud on the organisation's legislative and regulatory requirements?

f) How is the organisation able to negotiate contracts and agreements that fit its risk assessment and compliance environment?

g) What is the physical location of the data centre where your records are stored?

11. Measures to mitigate risks of managing records in the cloud.

a) How are your security considerations addressed in the Service Level Agreement (SLA)? **[ask to see a copy of the SLA]**

b) How can your organisation ensure the integrity, authenticity, and reliability of information stored in the cloud?

c) How does your organisation audit and monitor cloud services and establish relevant service-level agreements?

Last Question: Do you have any other comments about the use of cloud computing for records management in your organisation?

This is all I had to ask you. Is there anything you would like to ask me or comment about this interview? Thank you for your time and contribution to this research.

End of interview

APPENDIX F: INTERVIEW GUIDE FOR RECORDS MANAGEMENT STAFF

Instructions: Everything in bold is for the attention of the interviewer and not to be read out to the interviewee.

Interviewer introduce him/herself.

Interviewer hand over the consent form to the interviewee to sign.

g) Please briefly introduce yourself

h) Please briefly explain the work you do here?

i) How long have you been working here?

12. Reasons for adopting cloud computing for records management.

a) I understand your organisation is using cloud computing for records management, briefly explain your understanding of cloud computing?

b) Who was involved in the decision to use cloud computing for records management?

c) What are the reasons that led to the adoption of cloud computing for records management?

d) Which systems were used for records management before adopting cloud computing?

e) How are the previous systems integrated into the cloud solution adopted?

f) Are there cloud computing implementation policy documents? **[If yes, ask for copy. If no, ask what is used to guide the implementation of cloud computing].**

g) To what extend were you involved with preparations for cloud computing adoption?

13. Cloud computing services and deployment models.

a) Which service model(s) is your organisation using?

b) Which deployment model(s) is your organisation using?

14. Factors to consider when choosing a cloud service provider, service and deployment model(s).

a) Who was involved in deciding which cloud computing service(s) and deployment model(s) to use?

b) What are the reasons for choosing that service(s) and deployment model(s)?

c) Why did you choose that cloud service provider?

d) How do you collaborate with your IT department on cloud computing and to what extend?

15. The benefits of cloud computing for records management.

a) What are the benefits of cloud computing your organisation is experiencing?

b) To what extent is cloud computing a viable option for records management?

16. Risks of managing records in the cloud.

a) What are the challenges and risks associated with managing records in the cloud?

b) How does your organisation apply its records and information management programs to the cloud environment (retention schedules)? **[ask to be shown documentations of existing programs]**

c) What is the physical location of the data centre where your records are stored?

17. Measures to mitigate risks of managing records in the cloud.

a) How are your security considerations addressed in the Service Level Agreement (SLA)?

b) How does your organisation ensure the integrity, authenticity, and reliability of information stored in the cloud?

c) What is the impact of outsourcing services and information to the cloud on the organisation’s legislative and regulatory requirements?

d) How can the organisation apply its records and information management programs to the cloud environment?

e) Have you received any training about cloud computing?

f) If yes, what type of training did you receive; basic or technical training?

g) Have you used any of these publicly available guidelines on cloud computing for records management;

i. *Australian Digital Recordkeeping Initiative (ADRI) (2010) - 'Advice on Managing the Recordkeeping Risks associated with Cloud Computing'*

ii. *National Archives of Australia (2011) – 'A checklist for Records Management and the cloud'*

iii. *Archives and Records Association (UK & Ireland) (2010) - 'Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud.'*

h) If yes to question g), which one(s) and how were they helpful?

Last Question: Do you have any other comments about the use of cloud computing for records management in your organisation?

This is all I had to ask you. Is there anything you would like to ask me or comment about this interview? Thank you for your time and contribution to this research.

End of interview